Cookie Consents and Notices under the EU Data Protection Framework

Master's Thesis

19.05.2020

Alexandra From

Student ID: 014468861

University of Helsinki

Faculty of Law

Master's degree programme in International Business Law and Public International Law (MICL)

International Business Law

Supervisors: Riikka Koulu and Ville Pönkä

Tiedekunta – Fakultet – Faculty	**Koulutusohjelma – Utbildingsprogram – Degree Programme**
Faculty of Law	Master's degree programme in International Business Law and Public International Law (MICL)

Tekijä – Författare – Author
Alexandra From

Työn nimi – Arbetets titel – Title
Cookie Consents and Notices under the EU Data Protection Framework

Oppiaine/Opintosuunta – Läroämne/Studieinriktning – Subject/Study track
International Business Law / Communication and Information Law

Työn laji – Arbetets art – Level	**Aika – Datum – Month and year**	**Sivumäärä – Sidoantal – Number of pages**
Master's Thesis	May 2020	82

Tiivistelmä – Referat – Abstract

Data protection has become a pivotal topic in modern democratic societies. Lawmakers have, however, faced challenges in protecting data in the face of rapid technological growth and development in the online environment. 'Cookies' are a prominent tool for website operators that enable the collection and processing of vast amounts of personal data of internet users. The use of cookies is based on user's consent as required under Article 5(3) of Directive 2002/58/EC (ePrivacy Directive). It is, however, questionable whether cookie consent and notice practices are de facto effective in protecting internet users and providing them control over the use of their data obtained via cookies.

The goal of this master's thesis is to analyse whether the traditional model of consent and notice is the appropriate legal basis for the use of website cookies. The research question is divided into two parts. The first part concerns whether consent and notice are an effective tool in providing control and protection to individuals with respect to personal data processed through internet cookies. The second part concerns whether the EU's data protection framework provides clear and harmonised rules on cookie consents and notices. It will focus especially on the General Data Protection Regulation 2016/679 (GDPR) and the ePrivacy Directive. This thesis uses mainly the legal doctrinal method and qualitative empirical evidence in answering its research question.

After the introductory chapter, this thesis will in chapter 2 define cookies and its purposes, as well as outline the legal framework used in this research. Chapter 3 introduces the reader to the concept of consent and its different components, as well as the transparency principle and the accompanying information obligation. Consent consists of freely given, specific, informed and unambiguous elements. Chapter 4 will then discuss the first part of the research question. It will be seen that cookie consents and notices are burdened by many factors as evidenced through behavioural economics, cognitive and structural problems, as well as other factors. It is concluded, therefore, that cookie consents and notices in their traditional form are not an effective tool in providing control and data protection to internet users. Nevertheless, consent and notice are so enshrined in the EU's data protection regime that they will not be easily abandoned.

Chapter 5 discusses the second part of the research question by looking at practical examples in order to see how websites from the legal sector and different national data protection authorities have complied with cookie consent and notice obligations. It will be seen that cookie rules are interpreted inconsistently by even these websites, which has resulted in noncompliance in some instances. Hence, it is concluded that the GDPR and the ePrivacy Directive have failed to harmonise cookie consents and notices. Chapter 6 will look to the future and discuss briefly the proposed Regulation on Privacy and Electronic Communications (ePrivacy Regulation) in terms of i) 'cookie walls', which basically coerces website users to accept cookies or otherwise they will be denied access to the site or service, and ii) the legitimate interests ground, which has been introduced as an alternative legal basis to consent with respect to cookies in the latest revised draft of the ePrivacy Regulation adopted on 21 February 2020 by the Croatian Presidency. It will be concluded in chapter 7 that the traditional model of consent and notice might not always be the appropriate legal basis for cookies, hence legislators should look into other legal bases as well, such as, the legitimate interest ground. However, whether or not this ground will be able to provide better protection and control to internet users remains to be seen.

Avainsanat – Nyckelord – Keywords
Cookies, consent, privacy notice, cookie notice, transparency, GDPR, ePrivacy Directive, ePrivacy Regulation

Ohjaaja tai ohjaajat – Handledare – Supervisor or supervisors
Riikka Koulu and Ville Pönkä

Säilytyspaikka – Förvaringställe – Where deposited
Personal computer

Muita tietoja – Övriga uppgifter – Additional information

Table of Contents

Bibliography

Primary sources

Legislation

1. California Consumer Privacy Act 2018

2. Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

3. Convention for the Protection of Human Rights and Fundamental Freedoms 1950

4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37

6. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11

7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

8. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C 306/1

9. Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47

Cases - Court of Justice of the European Union

10. Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] OJ C 475

11. Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] OJ C 413

12. Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* [2019] OJ C 413, Opinion of AG Szpunar

13. Joined Cases C-397/01 to C-403/01 *Bernhard Pfeiffer and Others v Deutsches Rotes Kreuz, Kreisverband Waldshut eV* [2004] ECR 2004 I-08835

Secondary sources

Official Documents

14. Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (adopted on 21 November 2000) WP 37 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 20 February 2020

15. ——, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)' (adopted on 15 February 2007) WP 131 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf> accessed 20 February 2020

16. ——, 'Opinion 4/2007 on the Concept of Personal Data' (adopted on 20 June 2007) WP 136 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 17 April 2020

17. ——, 'Opinion 2/2010 on Online Behavioural Advertising' (adopted on 22 June 2010) WP 171 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 20 February 2020

18. ——, 'Opinion 15/2011 on the Definition of Consent' (adopted on 13 July 2011) WP 187 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed 20 February 2020

19. ——, 'Opinion 04/2012 on Cookie Consent Exemption' (adopted on 7 June 2012) WP 194 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 23 November 2019

20. ——, 'Opinion 02/2013 on Apps on Smart Devices' (adopted on 27 February 2013) WP 202 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> accessed 30 March 2020

21. ——, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (adopted on 2 October 2013) WP 208 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf> accessed 20 February 2020

22. ——, 'Cookie Sweep Combined Analysis - Report' (adopted on 3 February 2015) WP 229 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640605> accessed 26 February 2020

23. ——, 'Opinion 03/2016 on the Evaluation and Review of the EPrivacy Directive (2002/58/EC)' (adopted on 19 July 2016) WP 240 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf> accessed 20 February 2020

24. ——, ‘Opinion 01/2017on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)’ (adopted on 4 April 2017) WP 247 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140> accessed 20 February 2020

25. ——, ‘Guidelines on Consent under Regulation 2016/679’ (as last revised and adopted on 10 April 2018) WP 259 rev.01 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 26 February 2020

26. ——, ‘Guidelines on Transparency under Regulation 2016/679’ (as last revised and adopted on 11 April 2018) WP 260 rev.01 <https://iapp.org/media/pdf/resource_center/20180413_Article29WPTransparencyGuidelinespdf.pdf> accessed 26 February 2020

27. European Commission, ‘A Comprehensive Approach on Personal Data Protection in the European Union’ (Communication) COM (2010) 609 final

28. ——, ‘Stronger Protection, New Opportunities - Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018’ (Communication) COM (2018) 43 final

29. European Data Protection Board, ‘Statement of the EDPB on the Revision of the EPrivacy Regulation and Its Impact on the Protection of Individuals with Regard to the Privacy and Confidentiality of Their Communications’ (2018) <https://edpb.europa.eu/our-work-tools/our-documents/drugi/statement-edpb-revision-eprivacy-regulation-and-its-impact_en> accessed 7 May 2020

30. European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ COM (2017) 10 final

31. Council of the European Union, ‘Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ 2019 [12633/19]

32. ——, ‘Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ 2020 [5979/20]

33. ——, ‘Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ 2020 [6543/20]

34. Working Party on the Protection of Individuals with regard to the Processing of Personal data, ‘Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware’ (adopted on 23 February 1999) WP 17

<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf> accessed 20 February 2020

Literature

35. Atiyah PS, *The Rise and Fall of Freedom of Contract* (Clarendon Press 2003)

36. Benoist E, 'Collecting Data for the Profiling of Web Users' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008)

37. Betkier M, *Privacy Online, Law and the Effective Regulation of Online Services* (Intersentia 2019)

38. Borgesius FJZ, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163 <https://academic.oup.com/idpl/article/5/3/163/730611> accessed 21 February 2020

39. Borgesius FZ, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security Privacy 103 <https://ieeexplore.ieee.org/document/7085952> accessed 20 February 2020

40. Calo R, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2012) 87 Notre Dame Law Review 1027 <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/> accessed 18 February 2020

41. Carolan E, 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32 Computer Law & Security Review 462 <http://www.sciencedirect.com/science/article/pii/S0267364916300322> accessed 26 February 2020

42. Castelluccia C and others, 'Privacy Considerations of Online Behavioural Tracking' (European Network and Information Security Agency (ENISA) 2012) Report/Study <https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking> accessed 28 February 2020

43. Clifford D, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the Crumbs of Online User Behaviour' (2014) 5 JIPITEC <http://www.jipitec.eu/issues/jipitec-5-3-2014/4095> accessed 26 February 2020

44. Froomkin AM, 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461 <https://papers.ssrn.com/abstract=2715617> accessed 13 March 2020

45. Hildebrandt M, 'Profiling and the Identity of the European Citizen' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008)

46. Hildebrandt M and Tielemans L, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law & Security Review 509 <http://www.sciencedirect.com/science/article/pii/S0267364913001313> accessed 28 February 2020

47. Hirvonen A, *Mitkä metodit? Opas oikeustieteen metodologiaan* (Helsingin yliopisto, Oikeustieteellinen tiedekunta 2011)

48. Husa J, *Kirjoitetaan Juridiikkaa: Ohjeita Oikeustieteellisten Kirjallisten Töiden Laatijoille* (2., uud p, Talentum 2008)

49. Jones R and Tahri D, 'An Overview of EU Data Protection Rules on Use of Data Collected Online' (2011) 27 Computer Law & Security Review 630 <https://linkinghub.elsevier.com/retrieve/pii/S0267364911001488> accessed 25 March 2020

50. Kamp M, Körffer B and Meints M, 'Profiling of Customers and Consumers - Customer Loyalty Programmes and Scoring Practices' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008)

51. Koivisto I, 'The Anatomy of Transparency: The Concept and Its Multifarious Implications' (European University Institute 2016) Working Paper MWP 2016/09 <http://cadmus.eui.eu//handle/1814/41166> accessed 17 March 2020

52. ——, 'The IMF and the Transparency Turn' (2016) 25 Minnesota Journal of International Law 381 <https://heinonline.org/HOL/P?h=hein.journals/mjgt25&i=393> accessed 17 March 2020

53. Kolehmainen A, 'Tutkimusongelma Ja Metodi Lainopillisessa Työssä' in Tarmo Miettinen (ed), *Oikeustieteellinen opinnäyte: artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (Edita Publishing Oy 2016)

54. Koulu R, *Dispute Resolution and Technology: Revisiting the Justification of Conflict Management* (COMI 2016)

55. Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part I)' (2010) 18 International Journal of Law and Information Technology 176 <https://heinonline.org/HOL/P?h=hein.journals/ijlit18&i=180> accessed 13 March 2020

56. Leenes RE and Kosta E, 'Taming the Cookie Monster with Dutch Law - A Tale of Regulatory Failure' (2015) 31 Computer Law & Security Review 317 <http://www.sciencedirect.com/science/article/pii/S0267364915000059> accessed 26 February 2020

57. Leopold N and Meints M, 'Profiling in Employment Situations (Fraud)' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008)

58. Lindqvist J, *Personal Data Protection on the Internet of Things: An EU Perspective* (University of Helsinki, Faculty of Law 2018)

59. Lindroos-Hovinheimo S, *Miten Lakia Tulkitaan? – Erään Oikeusteoreettisen Kysymyksen Suomalaista Historiaa* (Lakimies 2011)

60. Mantelero A, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30

Computer Law & Security Review 643 <http://www.sciencedirect.com/science/article/pii/S026736491400154X> accessed 26 February 2020

61. Markou C, 'Behavioural Advertising and the New "EU Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer Netherlands 2016)

62. McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies' (2008) 4 ISJLP 543 <https://heinonline.org/HOL/P?h=hein.journals/isjlpsoc4&i=563> accessed 20 March 2020

63. Mitchell ID, 'Third-Party Tracking Cookies and Data Privacy' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2058326 <https://papers.ssrn.com/abstract=2058326> accessed 28 February 2020

64. Monteleone S, 'Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation' (2015) 43 Syracuse Journal of International Law and Commerce 69 <https://heinonline.org/HOL/P?h=hein.journals/sjilc43&i=71> accessed 25 February 2020

65. Richards N, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015)

66. Smits JM, 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2644088 <https://papers.ssrn.com/abstract=2644088> accessed 8 April 2020

67. Soh SY, 'Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour' (2019) 5 European Data Protection Law Review (EDPL) 65 <https://heinonline.org/HOL/P?h=hein.journals/edpl5&i=71> accessed 24 March 2020

68. Solove DJ, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880 <https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/> accessed 24 February 2020

69. Tene O and Polenetsky J, 'To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising' (2012) 13 Minn JL Sci & Tech 281 <https://heinonline.org/HOL/P?h=hein.journals/mipr13&i=281> accessed 20 March 2020

70. Zuiderveen Borgesius FJ and others, 'Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the EPrivacy Regulation' (2017) 3 European Data Protection Law Review (EDPL) 353 <https://heinonline.org/HOL/P?h=hein.journals/edpl3&i=382> accessed 31 March 2020

Newspaper Articles and Blogs

71. Baker J, 'How the EPrivacy Regulation Talks Failed ... Again' (26 November 2019) <https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/> accessed 29 November 2019

72. ——, 'Critics on Croatia's EPrivacy Proposal: Legitimate Interest Provisions Not Legitimate' (25 February 2020) <https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate/> accessed 7 May 2020

73. 'EPrivacy Regulation' (*e-Privacy European Regulation on Privacy and Electronic Communications,* last updated 30 March 2020) <https://cms.law/en/deu/insight/e-privacy> accessed 5 February 2020

74. 'EU Council Presidency Releases Proposed Amendments to Draft EPrivacy Regulation' (*Privacy & Information Security Law Blog*, 27 February 2020) <https://www.huntonprivacyblog.com/2020/02/27/eu-council-presidency-releases-proposed-amendments-to-draft-eprivacy-regulation/> accessed 1 April 2020

75. 'EU EPrivacy Regulation' (*IAPP Resource Center*) <https://iapp.org/resources/topics/eu-eprivacy-regulation/> accessed 5 February 2020

76. 'Facebook to Pay $5bn to Settle Privacy Concerns' *BBC News* (24 July 2019) <https://www.bbc.com/news/business-49099364> accessed 4 May 2020

77. Fazzini K, 'Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but so Far It's Mostly Created Frustration for Users, Companies, and Regulators' (*CNBC*, 5 May 2019) <https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html> accessed 6 May 2020

78. Ho V, 'Facebook's Privacy Problems: A Roundup' *The Guardian* (15 December 2018) <https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup> accessed 4 May 2020

79. Hodge R, 'Zoom Security Issues: Zoom Could Be Vulnerable to Foreign Surveillance, Intel Report Says' (*CNET,* 8 May 2020) <https://www.cnet.com/news/zoom-security-issues-zoom-could-be-vulnerable-to-foreign-surveillance-intel-report-says/> accessed 4 May 2020

80. Lohr S, 'Redrawing the Route to Online Privacy' *The New York Times* (27 February 2010) <https://www.nytimes.com/2010/02/28/technology/internet/28unbox.html> accessed 24 March 2020

81. Partington R, 'What Is Behavioural Economics?' *The Guardian* (9 October 2017) <https://www.theguardian.com/world/2017/oct/09/what-is-behavioural-economics-richard-thaler-nobel-prize> accessed 8 May 2020

82. Paul K, 'Worried about Zoom's Privacy Problems? A Guide to Your Video-Conferencing Options' *The Guardian* (9 April 2020) <https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives> accessed 4 May 2020

83. ‘The World’s Most Valuable Resource Is No Longer Oil, but Data’ *The Economist* (6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 6 May 2020

Other sources

84. ‘About EDPB’ (*European Data Protection Board - European Data Protection Board*, 10 January 2018) <https://edpb.europa.eu/about-edpb/about-edpb_en> accessed 8 May 2020

85. ‘Agencia Española de Protección de Datos | AEPD’ <https://www.aepd.es/es> accessed 17 February 2020

86. ‘Bird & Bird - International Law Firm’ (*Bird & Bird*) <http://www.twobirds.com/> accessed 17 February 2020

87. ‘Borenius’ (*Borenius*) <https://www.borenius.com/> accessed 17 February 2020

88. ‘Cookies’ (8 January 2020) <https://ico.org.uk/global/cookies/> accessed 3 March 2020

89. ‘Cookies Policy’ (*Bird & Bird*) <http://www.twobirds.com/en/more-information/cookies-policy> accessed 27 April 2020

90. ‘Data Protection Authority’ <https://www.dataprotectionauthority.be/> accessed 17 February 2020

91. Datainspektionen, ‘Datainspektionen’ <https://www.datainspektionen.se/> accessed 3 March 2020

92. ‘Deloitte | Audit, Consulting, Financial, Risk Management, Tax Services’ (*Deloitte*) <https://www2.deloitte.com/global/en.html> accessed 17 February 2020

93. Digital Power, ‘What Is a Cookie?’ (21 June 2012) <https://www.youtube.com/watch?v=I01XMRo2ESg> accessed 18 February 2020

94. ‘Digital Single Market – Stronger Privacy Rules for Electronic Communications’ (*European Commission - European Commission,* 10 January 2017) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_17> accessed 15 April 2020

95. European Commission, ‘Flash Eurobarometer 443: E-Privacy, Full Report’ (2016) <https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy> accessed 31 March 2020

96. ——, ‘Special Eurobarometer 487a: The General Data Protection Regulation, Full Report’ (2019) <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222> accessed 4 April 2020

97. Fieldfisher, ‘Cookie “Consent” Rule: EEA Implementation’ (Field Fisher Waterhouse) <https://res.cloudinary.com/fieldfisher/image/upload/v1574345727/PDF-

Files/PDFs%20from%20old%20website/EU-Cookie-Consent-Tracking-Table-Fieldfisher-21-April-2015_fzwqve.pdf> accessed 18 February 2020

98. 'GDPR Enforcement Tracker - List of GDPR Fines' <http://www.enforcementtracker.com> accessed 2 March 2020

99. 'GDPR in Numbers' (European Commission, 22 May 2019) <https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf> accessed 4 April 2020

100. 'GDPR in Numbers' (European Commission, 25 January 2019) <https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf> accessed 22 April 2020

101. 'Hannes Snellman - Home' <https://www.hannessnellman.com/> accessed 17 February 2020

102. 'Homepage | CNIL' <https://www.cnil.fr/en/home> accessed 17 February 2020

103. 'Homepage | Data Protection Commission' (*Homepage | Data Protection Commission*) <https://www.dataprotection.ie/> accessed 22 April 2020

104. 'Information Commissioner's Office' (12 February 2020) <https://ico.org.uk/> accessed 17 February 2020

105. 'Microsoft Privacy Statement – Microsoft Privacy' <https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodule> accessed 28 February 2020

106. Moerel L, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' (Lecture at Tilburg University, 14 February 2014) <https://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf> accessed 2 March 2020

107. Organisation for Economic Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013) <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> accessed 22 February 2020

108. 'Roschier - Leading Law Firm in the Nordic Region' (*Roschier*) <https://www.roschier.com/> accessed 17 February 2020

109. 'Synopsis Report of the Public Consultation on the Evaluation and Review of the EPrivacy Directive' (European Commission 2016) <https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive> accessed 18 September 2019

110. 'Tietosuojavaltuutetun toimisto' (*Tietosuojavaltuutetun toimisto*) <https://tietosuoja.fi/etusivu> accessed 3 March 2020

111. TRUSTe and Fieldfisher, ‘EU Cookie Audits: Are You Ready?’ <https://iapp.org/resources/article/eu-cookie-audits-are-you-ready/> accessed 18 February 2020

112. Wainer L and others, ‘Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management’ (Joint Research Centre and European Commission 2012) JRC Scientific and Policy Reports <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/pan-european-survey-practices-attitudes-and-policy-preferences-regards-personal-identity> accessed 25 February 2020

113. ‘What Are Cookies and Similar Technologies?’ (*Information Commissioner’s Office*, 14 November 2019) <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/> accessed 23 November 2019

Abbreviations

AEPD
- Agencia Española de Protección de Datos (Spanish data protection authority).

AG
- Advocate General.

APD-GBA
- Autorité de la protection des données – Gegevensbeschermingsautoriteit (Belgian data protection authority).

Charter
- Charter of Fundamental Rights of the European Union.

Citizens' Rights Directive
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

CJEU
- Court of Justice of the European Union.

CNIL
- Commission Nationale de l'Informatique et des Libertés (French data protection authority).

Data Protection Directive
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EDPB
- European Data Protection Board.

EEA
- European Economic Area.

ePrivacy Directive
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

ePrivacy Regulation
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic

communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

EU
- European Union.

EU Council Presidency
- Presidency of the Council of the European Union.

GDPR/ the Regulation
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

ICO
- Information Commissioner's Office (The UK's data protection authority).

Planet49
- Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH.*

WP29
- Article 29 Data Protection Working Party.

1 Introduction

Having information about others equals power.[1] Due to the 'rapid growth of privacy-destroying technologies' privacy and protection of personal data is endangered not only by government surveillance, but also by private sector monitoring,[2] especially in the online environment. This phenomenon has been called 'multiveillance', which means 'surveillance not just by the state but by companies, marketers, and those in our social networks'.[3] Though, privacy and data protection have long been recognised as important and fundamental principles in the modern world,[4] lawmakers seem to have had challenges to keep up with the rapid technological developments and protecting privacy and personal data in the online environment. This can be seen from the fact that online data protection in the European Union (hereafter the 'EU') is still regulated by almost a two decades old legal instrument, the Directive 2002/58/EC (hereafter the 'ePrivacy Directive'),[5] which has been amended once during this period.[6]

Privacy and protection of personal data are fundamental human rights in the EU and incorporated in its legislations. The Charter of Fundamental Rights of the European Union (hereafter the 'Charter'), which is legally binding on all EU Member States,[7] embraces these rights in Articles 7 and 8 respectively.[8] The Treaty on the Functioning of the European Union,[9] which is one of the two pillars of the EU's constitution, includes also the right to the protection of personal data in Article 16(1).[10] The EU's data protection regime allows, however, the

[1] A Michael Froomkin, 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461, 1462 <https://papers.ssrn.com/abstract=2715617> accessed 13 March 2020.
[2] ibid 1463, 1465.
[3] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015) 5.
[4] Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part I)' (2010) 18 International Journal of Law and Information Technology 176, 176–177 <https://heinonline.org/HOL/P?h=hein.journals/ijlit18&i=180> accessed 13 March 2020.
[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.
[6] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11.
[7] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C 306/1 Article 6.
[8] Charter of Fundamental Rights of the European Union [2000] OJ C 364/1.
[9] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47; see also Treaty of Lisbon.
[10] see also Convention for the Protection of Human Rights and Fundamental Freedoms 1950 Article 8 which also enshrines the right to privacy.

processing of personal data in accordance with law, while at the same time striving to employ high level of safety and security requirements to justify the interference with these fundamental rights. One such legislation is the famous General Data Protection Regulation (hereafter the 'GDPR' or the 'Regulation'),[11] which came into force on 25 May 2018 and repealed and replaced Directive 95/46/EC (hereafter the 'Data Protection Directive').[12]

The European Commission has also proposed a supplementary legislation to the GDPR that will provide specific rules with respect to privacy and data protection in the electronic communications sector. The forthcoming *lex specialis* Regulation on Privacy and Electronic Communications (hereafter the 'ePrivacy Regulation')[13] is still a work in progress and has been revised under the different Presidencies of the Council of the European Union (hereafter the 'EU Council Presidency').[14] At the time of writing this thesis, the newest revised version of the draft ePrivacy Regulation was adopted on 21 February 2020 by the Croatian Presidency.[15] The much awaited ePrivacy Regulation was supposed to come into force at the same time as the GDPR, so that the EU would have an updated and comprehensive data protection framework in place.[16] As a result of the delay the ePrivacy Directive,[17] as amended,[18] remains still in force as the *lex specialis* law to the GDPR.[19] It will be repealed by the proposed ePrivacy Regulation once in force, though at the moment it seems that its enactment might be pushed to even so far as 2023.[20]

---

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
[13] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final.
[14] see for example 'EPrivacy Regulation' (*e-Privacy European Regulation on Privacy and Electronic Communications,* last updated 30 March 2020) <https://cms.law/en/deu/insight/e-privacy> accessed 5 February 2020 and; 'EU EPrivacy Regulation' (*IAPP Resource Center*) <https://iapp.org/resources/topics/eu-eprivacy-regulation/> accessed 5 February 2020.
[15] 'EU Council Presidency Releases Proposed Amendments to Draft EPrivacy Regulation' (*Privacy & Information Security Law Blog*, 27 February 2020) <https://www.huntonprivacyblog.com/2020/02/27/eu-council-presidency-releases-proposed-amendments-to-draft-eprivacy-regulation/> accessed 1 April 2020.
[16] see 'Digital Single Market – Stronger Privacy Rules for Electronic Communications' (*European Commission - European Commission,* 10 January 2017) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_17> accessed 15 April 2020.
[17] ePrivacy Directive.
[18] Citizens' Rights Directive.
[19] European Commission, 'Stronger Protection, New Opportunities - Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018' (Communication) COM (2018) 43 final.
[20] 'EPrivacy Regulation' (n 14).

The internet has been described as 'an international network of interconnected computers, which enables millions of people to communicate with one another in "cyberspace" and to access vast amounts of information from around the world'.[21] As the use of internet has expanded in the 21st century, the privacy risks inherent in this kind of 'open network' also emerge.[22] People are rarely aware of the massive volume of data that is collected and processed about them when they access and surf the internet, hence they are being robbed of their freedom to make decisions regarding the use of their personal data.[23] The internet has traditionally employed this kind of invisible processing through 'privacy-invading features',[24] due to fast data flows and by disregarding the rules on informing the users about the processing operations and purposes.[25] It is important that information about the processing of personal data is brought to the attention of internet users as this concerns their fundamental human rights. The EU has recognised the importance of protecting privacy and personal data also in the online environment and therefore personal data protection is no longer a 'niche area' but has extended its embrace to almost all fields of law.[26]

Websites and mobile applications use 'cookies', which are a type of technology that enables the invisible processing of user's data.[27] It is 'a computer record of information that is sent from a web server to an user's computer for the purpose of future identification of that computer on future visits to the same web site'.[28] Cookies can be used for a range of purposes, such as, profiling the internet user in order to provide targeted advertisements on the internet.[29] Cookies can thus be very intrusive and contain high-privacy risks. The Article 29 Data

[21] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (adopted on 21 November 2000) WP 37 8 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 20 February 2020.
[22] ibid 13.
[23] ibid 47, 73.
[24] Working Party on the Protection of Individuals with regard to the Processing of Personal data, 'Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware' (adopted on 23 February 1999) WP 17 4 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf> accessed 20 February 2020.
[25] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 47.
[26] Kuner (n 4) 176.
[27] Working Party on the Protection of Individuals with regard to the Processing of Personal data (n 24) 4; Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (adopted on 27 February 2013) WP 202 12 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> accessed 30 March 2020.
[28] Working Party on the Protection of Individuals with regard to the Processing of Personal data (n 24) 4.
[29] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 73.

Protection Working Party (hereafter the 'WP29') has recognised that the 'Internet is not just a worldwide information platform, but also a worldwide market place where competing businesses try to attract potential customers'.[30] Thus, though protecting user's personal data is crucial as part of their fundamental human rights, the data protection rules must be balanced against companies' economic interests.[31]

The WP29 has been reformed since the GDPR came into force and is now known as the European Data Protection Board (hereafter the 'EDPB').[32] It is an independent body that has an advisory role in the EU's data protection framework.[33] It consists of the heads of the national data protection authorities from each Member State.[34] The WP29's opinions, guidelines and recommendations on the interpretation of the data protection concepts and rules, most of which have been endorsed by the EDPB, are not legally binding.[35] Nevertheless, as they are an advisory body and one of their functions is to facilitate a harmonised interpretation of the EU's data protection laws,[36] companies and organisations are recommended to take into account their opinions and guidelines when implementing data protection rules.

Consent is an important concept in data protection and provides one of the justifications for the interference with this fundamental right. For example, the Charter has explicitly recognised that personal data can be processed only 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[37] Consent is also one of the legal bases under Article 6(1) of the GDPR that makes processing of personal data lawful. It does not, however, take precedence over the other available legal bases in the provision.[38] Controllers should consider on a case by case basis, which one of the six options under Article 6(1) will be the most appropriate legal ground for the processing in question.[39] It should be noted, however,

[30] ibid 73.
[31] ibid 19.
[32] see GDPR Article 68.
[33] see Data Protection Directive Article 29; GDPR Articles 68-70; 'About EDPB' (*European Data Protection Board - European Data Protection Board*, 10 January 2018) <https://edpb.europa.eu/about-edpb/about-edpb_en> accessed 8 May 2020.
[34] see Data Protection Directive Article 29; GDPR Article 68.
[35] see 'About EDPB' (n 33).
[36] GDPR Article 70; Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 90.
[37] the Charter Article 8(2).
[38] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (adopted on 13 July 2011) WP 187 7–8 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed 20 February 2020.
[39] ibid.

that Article 5(3) of the ePrivacy Directive has made consent a prerequisite before cookies can be placed on a user's device. The legislator's decision to use consent for cookies has sparked criticism and debate among scholars on whether consent is de facto effective in protecting personal data in the online environment.[40] Another issue with the ePrivacy Directive is that as EU directives must be implemented into national law by each Member State, this generally results in some varying rules and differing interpretations of the EU law on national level.[41] Thus, the definition of what amounts to valid 'consent' with respect to cookies may also vary between Member States.[42]

Transparency is also a pivotal principle in the EU data protection law.[43] It is a principle in itself but also part of the conditions for a valid consent, since a data subject must be informed of the processing of personal data, before he or she can provide an effective consent under the GDPR and the ePrivacy Directive.[44] Thus, consent must be based on prior information. Providing transparency is deemed to invoke user's trust and better data protection as it is easier to hold companies accountable for misconduct.[45] On the other hand, too much transparency can also be overwhelming and as a result become an obstacle in ensuring good data protection. For instance, academics have criticised transparency as being deceptive and they have considered it as one of the stumbling blocks in obtaining valid consent.[46]

---

[40] see for example Marcin Betkier, *Privacy Online, Law and the Effective Regulation of Online Services* (Intersentia 2019); Frederik Zuiderveen Borgesius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security Privacy 103 <https://ieeexplore.ieee.org/document/7085952> accessed 20 February 2020; Sheng Yin Soh, 'Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour' (2019) 5 European Data Protection Law Review (EDPL) 65 <https://heinonline.org/HOL/P?h=hein.journals/edpl5&i=71> accessed 24 March 2020; Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law & Security Review 643 <http://www.sciencedirect.com/science/article/pii/S026736491400154X> accessed 26 February 2020.

[41] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 36.

[42] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (adopted on 2 October 2013) WP 208 3 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf> accessed 20 February 2020.

[43] see for example Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (as last revised and adopted on 11 April 2018) WP 260 rev.01 para 2 <https://iapp.org/media/pdf/resource_center/20180413_Article29WPTransparencyGuidelinespdf.pdf> accessed 26 February 2020.

[44] see GDPR Articles 4(11) and 5(1)(a); ePrivacy Directive Article 5(3).

[45] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 2 and 4.

[46] see for example Jenna Lindqvist, *Personal Data Protection on the Internet of Things: An EU Perspective* (University of Helsinki, Faculty of Law 2018); Ida Koivisto, 'The Anatomy of Transparency: The Concept and Its Multifarious Implications' (European University Institute 2016) Working Paper MWP 2016/09 <http://cadmus.eui.eu//handle/1814/41166> accessed 17 March 2020; Ryan Calo, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2012) 87 Notre Dame Law Review 1027 <https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/> accessed 18 February 2020; Eoin Carolan, 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32 Computer Law

1.1 RESEARCH QUESTION, STRUCTURE AND SCOPE

The overarching research question for this thesis is *whether or not the traditional model of consent and notice is the appropriate legal basis for the use of cookies*. The research question is divided into the following parts:

i) Are consent and notice an effective tool in providing control and protection to individuals in the context of personal data processed through internet cookies?

ii) Does the GDPR and the ePrivacy Directive provide clear and harmonised rules on cookie consents and notices?

The focus of this thesis is website cookies used on computers. It does not include in its scope cookies used in applications downloaded on mobile devices. This research discusses cookies in general and does not distinguish between the different uses, though some scholarly articles used in this thesis as source material focus mainly on cookies used for online tracking or behavioural advertising. These include articles by authors, such as, professor Borgesius,[47] researcher Clifford,[48] and professors Tene and Polonetsky.[49] Additionally, the thesis will focus only on the general issue of consent and transparency with respect to cookies and will not consider any special areas, such as, children or vulnerable people. Furthermore, the notion of consent as used in other fields of law, such as, contract law is not included in the scope of this research as the research is restricted to data protection. This thesis will use the term 'regular consent' when distinguishing Article 6(1)(a) consent from Article 9(2)(a) 'explicit consent' of the GDPR. Furthermore, the analysis on the effectiveness of privacy notices in subchapter 4.2. is used as a reflection on the issue of traditional notices in general including cookie notices.

After this introductory chapter the thesis will present in chapter 2 the definition and purposes of cookies and outline the legal framework examined in this thesis. In chapter 3 the reader is

& Security Review 462 <http://www.sciencedirect.com/science/article/pii/S0267364916300322> accessed 26 February 2020.

[47] Borgesius (n 40); Frederik J Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163 <https://academic.oup.com/idpl/article/5/3/163/730611> accessed 21 February 2020.

[48] Damian Clifford, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the Crumbs of Online User Behaviour' (2014) 5 JIPITEC <http://www.jipitec.eu/issues/jipitec-5-3-2014/4095> accessed 26 February 2020.

[49] Omer Tene and Jules Polenetsky, 'To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising' (2012) 13 Minn JL Sci & Tech 281 <https://heinonline.org/HOL/P?h=hein.journals/mipr13&i=281> accessed 20 March 2020.

introduced to the concept of consent and the principle of transparency. Subchapters 3.1-3.6 discuss consent, its different components and supplementary elements. The requirements of valid consent have not changed drastically as the main elements are still freely given, specific, informed and unambiguous indication, but the GDPR has clarified that active behaviour is key. There is, however, some ambiguity between the difference of 'regular consent' under Article 6(1)(a) and 'explicit consent' under Article 9(2)(a) of the GDPR, which is explored in subchapter 3.7. This thesis will then introduce in subchapters 3.8 and 3.9 the transparency principle and controller's information obligation respectively, which in essence is the tool to comply with the transparency principle under the data protection regime. Subchapter 3.10 provides a short conclusion to the chapter.

Chapter 4 will discuss whether or not consent and notice provide an effective protection mechanism to internet users with respect to cookies. It will be seen that cookie consents and notices are burdened by many factors as evidenced by behavioural economics, cognitive and structural problems, as well as other factors. It is concluded, therefore, that cookie consents and notices in their traditional form are not an effective tool in providing control and data protection to internet users. Hence, consent and notice might not always be the appropriate legal basis for processing data obtained through cookies. Nevertheless, consent and notice are so enshrined in the EU's data protection regime that they seem to be here to stay. This thesis is, however, not of the opinion that consent should be disregarded altogether with respect to cookies, but that the consent and notice mechanisms should be improved.

Chapter 5 will then look at practical examples to see how and if websites have complied with cookie consent and notice obligations. It will be seen that cookie rules are interpreted inconsistently by websites, which has resulted in noncompliance in some instances. Hence, it can be inferred from the results that the GDPR and the ePrivacy Directive have, at least to a certain extent, failed to harmonise cookie consents and notices. Therefore, there is room for improvement in terms of clarifying and harmonizing cookie rules. Additionally, some websites do not provide a real choice when requesting consent, hence data subject's control over his or her personal data becomes illusory. Thus, it is questionable whether another legal basis, such as, legitimate interest might be more suitable in these circumstances.

Chapter 6 will look at the future of cookie regulation in terms of discussing briefly the proposed ePrivacy Regulation to the extent that it is applicable to the discussion of website cookies. It

will look more closely at the issue with 'cookie walls', which basically coerces website users to accept cookies or otherwise they will be denied access to the site or service. This thesis will argue that cookie walls should be prohibited completely, with strict exceptions if needed, since it is unfair to force user's hand in accepting cookies. This could not be considered as freely given consent. The latest revised draft of the ePrivacy Regulation has introduced an alternative legal basis to consent for cookies, which is the legitimate interest ground. This thesis applauds the EU Council Presidency for its efforts to bring forth another legal basis with regards to the use of cookies, since consent might not always be an effective tool nor the appropriate one. Lastly, chapter 7 will provide an overall conclusion to this thesis.

1.2 METHODOLOGY AND SOURCES

This thesis is a research of the legal doctrine of the EU's data protection law focusing mainly on the provisions and recitals of the GDPR and the ePrivacy Directive, hence contributing to the *de lege lata*[50] discussion of these two important legal instruments on the EU level. Accordingly, this thesis uses mainly the legal doctrinal method. This thesis provides also some discussion on the *de lege ferenda*[51] proposed ePrivacy Regulation to the extent that it is applicable to the discussion of website cookies in this thesis. Thus, the research will not provide an in-depth analysis of the draft ePrivacy Regulation as a whole but will look at it only within the parameters of this thesis' topic.

Legal doctrine has been described as 'research that aims to give a systematic exposition of the principles, rules and concepts governing a particular legal field or institution and analyses the relationship between these principles, rules and concepts with a view to solving unclarities and gaps in the existing law'.[52] The centre of legal doctrinal method is the analysis of existing law and the content of its legal norms,[53] in order to explore how citizens should de facto act within

[50] Antti Kolehmainen, 'Tutkimusongelma Ja Metodi Lainopillisessa Työssä' in Tarmo Miettinen (ed), *Oikeustieteellinen opinnäyte: artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (Edita Publishing Oy 2016) 108. Kolehmainen stated that when interpreting de lege lata legislation the 'interpretation recommendations are based on the sources of law doctrine'.
[51] ibid. When interpreting de lege ferenda legal instruments, Kolehmainen stated that 'reflections can be made more freely, for example on the basis of a consideration of social expediency'.
[52] Jan M Smits, 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2644088 5 <https://papers.ssrn.com/abstract=2644088> accessed 8 April 2020.
[53] Ari Hirvonen, *Mitkä metodit? Opas oikeustieteen metodologiaan* (Helsingin yliopisto, Oikeustieteellinen tiedekunta 2011) 21–22.

a legal system in accordance with the law.[54] The purpose of legal doctrine is to interpret and systematise law.[55] Systematisation provides both a practical and theoretical dimension to legal doctrine, which are interlinked.[56] This thesis will discuss the issue of consent and transparency in the online environment with respect to internet cookies on a theoretical and practical level, thereby providing a comparison between law in books and law in action.

Concrete examples of website cookie consent and notice mechanisms are used through screenshots in order to demonstrate law in action. This is not a quantitative empirical research due to the limited amounts of examples used. Instead this thesis uses qualitative empirical evidence in order to support its hypothesis. The thesis examines the cookie consent requests in the examples, but it will not provide an in-depth analysis of the full cookie notices. Instead, it will look more at the compact text accompanying the cookie consent requests, as this tends to be the first information that users see with respect to cookies.

Due to limited space only ten examples are used, five for each category. The websites selected are a) national data protection authorities and b) law firms in Finland, in order to show that even among law firms in Finland and data protection authorities across the EU there is, to a certain extent, a lack of consensus with respect to cookie practices. The examples support the second hypothesis regarding the inconsistency of cookie consents and notices, despite harmonization attempts by the GDPR and the ePrivacy Directive. This thesis does acknowledge that the results are limited, since the selected websites represent only the legal sector and public supervisory authorities. Social media platforms, newspaper sites and third party advertisers could have provided additional insight into the diverse cookie practices and cookie compliance issues in other sectors. The above mentioned websites were chosen, however, because this thesis considers it interesting to examine how the legal sector and the public supervisory authorities have interpreted and tackled this issue of cookies and cookie consent requests, especially since they are the ones giving companies and organisations legal advice and enforcing the rules respectively.

[54] Jaakko Husa, *Kirjoitetaan Juridiikkaa: Ohjeita Oikeustieteellisten Kirjallisten Töiden Laatijoille* (2., uud p, Talentum 2008) 20.
[55] Hirvonen (n 53) 22.
[56] ibid 25.

The national data protection authorities were chosen on the basis that a) they use cookies,[57] and b) in order to show how data protection authorities in different parts of the EU have reacted and implemented cookie consent mechanisms. It will be seen that there is some discrepancy in the implementations. This inconsistency is burdensome for companies and organizations who operate on a multinational level, because their websites in different countries must also adhere to the local laws. If the Member States are not in consensus of what constitutes the correct cookie practices under the EU data protection laws, then this will be very onerous on the companies, who must tailor their cookie practices in accordance with all the national laws where they operate their websites. Additionally, the fact that even law firms in Finland apply different cookie practices may very well result in the giving of different advices to companies on cookie policies and practices within the country. The law firms were chosen on the basis that they are multinational in nature but have at least one office in Finland, in order to show that even big law firms interpret cookie rules differently.

Legal interpretation is a key method in legal doctrine.[58] Nevertheless, interpretation suffers always from some level of bias and can thus never be completely objective.[59] This thesis applies legal interpretation in its analysis of the legal norms in the EU's data protection regime using legal sources as the basis for its legal construction. Legal sources have different levels of weight in the legal doctrine depending on the category that they fall in to.[60] In the Finnish legal system legal sources are commonly divided into a) strongly binding, which include, inter alia, legislation and case law of the Court of Justice of the European Union (hereafter the 'CJEU'), b) weakly binding, such as, legislative preparatory documents, and c) permitted legal sources, such as, general legal principles, ethical and moral principles and comparative arguments.[61]

This thesis uses WP29's opinions and guidelines, since they have an advisory role in the data protection framework by interpreting the provisions in the EU's data protection legislations and providing clarifications and best practices. Additionally, this thesis makes use of academic

[57] Not all supervisory authorities use cookies on their websites, e.g. the Finnish and the Irish data protection authorities do not use cookies, at least at the time of writing this thesis. See 'Tietosuojavaltuutetun toimisto' (*Tietosuojavaltuutetun toimisto*) <https://tietosuoja.fi/etusivu> accessed 3 March 2020; 'Homepage | Data Protection Commission' (*Homepage | Data Protection Commission*) <https://www.dataprotection.ie/> accessed 22 April 2020.
[58] Hirvonen (n 53) 36.
[59] ibid 37; Susanna Lindroos-Hovinheimo, *Miten Lakia Tulkitaan? – Erään Oikeusteoreettisen Kysymyksen Suomalaista Historiaa* (Lakimies 2011) 297.
[60] Kolehmainen (n 50) 116.
[61] ibid 116–117.

debate surrounding consent and transparency, in order to give teeth to the discussion and criticism of their legal complexities in the online environment. When interpreting the notions of consent and transparency this thesis uses constructive method, which is applicable when deducing concepts in legal doctrine.[62]

The purpose of comparative law is to analyse distinct legal systems or national laws and it is an independent legal area,[63] though it can also be used as a support tool in the legal doctrinal method.[64] This thesis will focus on EU law and will not include in its scope national implementations of EU legal instruments. Hence, this thesis will not incorporate comparative law method in its sphere of study. Nevertheless, as mentioned above, this thesis does use cookie practices of different national data protection authorities as part of its qualitative empirical evidence in order to demonstrate law in action, but it will not provide a comparison or an in-depth analysis of the distinct national laws.

[62] Hirvonen (n 53) 45.
[63] ibid 26.
[64] Husa (n 54) 23.

2 Cookies

2.1 DEFINITION AND PURPOSE OF COOKIES

Cookies have been described as 'pieces of data that can be stored in text files that may be put on the internet user's hard disk, while a copy may be kept by the website'.[65] The cookie will then stay on the user's device for the amount of time that the cookie is programmed to and collect information about the user for the website's different purposes.[66] Cookies can collect information about, for example, the pages the user has viewed, advertisements that have been clicked and any other information that the website is interested in knowing about the user.[67] Some cookies have a more practical role, such as, enabling the proper functioning of the website, or facilitating the services provided by the website,[68] or combatting fraud and abuse.[69] Cookies are also used to remember, for example, language preferences, items in the shopping basket[70] and other actions or preferences conducted on the website by the user or visitor.[71]

Cookies may be considered invasive, because they can contain a unique id that is stored on the user's computer and that recognises the user whenever he or she returns to the website.[72] Thus, cookies enable 'invisible processing' of user's personal data by website operators without the user's knowledge.[73] The unique identifier in cookies enables the personalisation of website user's information[74] and thus the website can 'keep track of a user's patterns and preferences'.[75] Due to this, cookies can also be used to create online user profiles for the purpose of targeted advertisement on the internet.[76] As Clifford has stated 'tracking and the resulting profiling have become a key part of the business model of many Web 2.0 services'.[77] This is because targeted

[65] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 16.
[66] ibid.
[67] ibid.
[68] ibid.
[69] see for example 'Microsoft Privacy Statement – Microsoft Privacy' <https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodule> accessed 28 February 2020.
[70] Digital Power, 'What Is a Cookie?' (21 June 2012) <https://www.youtube.com/watch?v=I01XMRo2ESg> accessed 18 February 2020.
[71] Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* [2019] OJ C 413, Opinion of AG Szpunar, para 37.
[72] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 16, 42; Digital Power (n 70).
[73] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 21.
[74] ibid 42.
[75] ibid 93.
[76] ibid 73.
[77] Clifford (n 48) 194.

advertisement is a financial resource to website service providers, which enables them to offer many of their online services without monetary payment but instead in exchange for the user's personal data.[78]

There are different types of cookies and some are distinguished by their duration.[79] 'Session cookies' are cookies that exist during the browser session and are 'automatically deleted when the user closes his browser'.[80] Hence, they are less intrusive than persistent cookies.[81] 'Persistent cookies', on the other hand, are stored on the user's device until their programmed expiration date.[82] Persistent cookies can last for minutes, days, or even several years.[83] Retention periods that last for several years can be considered as unreasonably long.[84] Persistent cookies enable user's actions or preferences to be recollected 'across a site (or across different websites)', hence are more intrusive.[85] The Cookie Sweep Combined Analysis report, conducted by the WP29 in 2015, showed that the participating websites used a lot more persistent cookies than session cookies with a ratio of about 86% and 14% respectively.[86]

Cookies can also be differentiated by their domain, such as, first party and third party cookies.[87] First-party cookies are those cookies that a business stores and reads 'on its *own* website'.[88] These type of cookies are usually functional in nature, for example, they store information

[78] Borgesius (n 40) 103.
[79] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 42.
[80] Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (adopted on 7 June 2012) WP 194 4 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 23 November 2019.
[81] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 42, 80.
[82] Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (n 80) 4.
[83] ibid; see also Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis - Report' (adopted on 3 February 2015) WP 229 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640605> accessed 26 February 2020. The report found that the longest cookie was set to 7991 years and some were set to over 100 and 1000 years. As for third party cookies the longest was set for 7985 years and some were set for over 68 years and others for over 10 years. However, if the cookies with over 100 years of duration are excluded, the average lifespan of a cookie was nevertheless 1-2 years.
[84] Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis' (n 83) 19.
[85] 'What Are Cookies and Similar Technologies?' (*Information Commissioner's Office*, 14 November 2019) <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/> accessed 23 November 2019.
[86] Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis' (n 83) 8.
[87] Opinion of AG Szpunar in *Planet49* (n 71) para 40.
[88] Christina Markou, 'Behavioural Advertising and the New "EU Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer Netherlands 2016) 216 original emphasis.

about user's preferences, for example, login details[89] or language preferences.[90] Third party cookies are, on the other hand, cookies that are stored by a third party, usually an advertising network agency, who has made agreements with various websites and shows advertisements on those websites.[91] The results from the Cookie Sweep Combined Analysis report showed that 70% of cookies used by the 478 participating websites were third party cookies.[92] Third-party cookies are more privacy invasive than first-party cookies, because they 'track users across a number of websites and collect information on their behaviour in multiple domains. As a result, they enable the construction of particularly detailed user profiles'.[93]

As seen from the survey, website operators tend to use the more privacy intrusive cookies. This could be considered as evidence of deficient data protection rules in terms of cookies, which has resulted in the common use of privacy invasive cookie technology by website services. Nevertheless, though cookies can be intrusive they can also be very useful as discussed above. Even the WP29 has acknowledged that some cookies may be necessary and thus rejecting 'all *cookies* might not be in the interest of the Internet user'.[94] Furthermore, though cookies can contain massive amount of information about the user to whom it attaches the unique identifier to, only the website placing the cookie on the user's computer can read it.[95]

2.2 COOKIE REGULATION IN THE EU

2.2.1 The GDPR

The GDPR came into force on 25 May 2018 and is a *lex generalis* legislation concerning the protection of personal data. The Regulation is applicable to both offline and online processing of personal data.[96] Any data that is categorised as 'personal data' will fall under the scope of the GDPR, subject to few exceptions, such as, if individual processes personal data for purely household reasons.[97] The definition of personal data under the GDPR is wide and encompasses any information that relates to an 'identified or identifiable natural person', in other words, the

[89] Clifford (n 48) 195.
[90] see for example 'Microsoft Privacy Statement – Microsoft Privacy' (n 69).
[91] Markou (n 88) 216.
[92] see Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis' (n 83) 2, 5 and 6.
[93] Markou (n 88) 216.
[94] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (n 21) 80 original emphasis.
[95] Digital Power (n 70).
[96] see GDPR Article 2.
[97] see ibid.

data subject, whether directly or indirectly.[98] Online identifiers are explicitly mentioned in the provision as examples of 'personal data'.[99]

As mentioned above, cookies can contain identification numbers that remember the user's device and they can contain a lot of information about the user. Thus, cookies tend to process personal data.[100] Consequently, the GDPR applies also to data processed via cookies if such data falls under the concept of personal data. Furthermore, the WP29 recognised already under the Data Protection Directive that identification of a person can be achieved, not just by knowing a person's name but also 'when other "identifiers" are used to single someone out'.[101] Thus, this interpretation seems to have covered cookie identifiers in its definition of personal data already in the pre-GDPR era.

2.2.2 The ePrivacy Directive

The ePrivacy Directive, which came into force on 31 July 2002, is a *lex specialis* legislation to the GDPR as it regulates privacy in the electronic communications sector.[102] It covers also the use of cookies and similar devices, which are permitted, provided that they have a legitimate purpose and users must be aware of such use.[103] The ePrivacy Directive is applicable to cookies regardless if the cookie data is considered personal data or not. This is confirmed by Recital 24, which states that users' device and any information that it contains are 'part of the private sphere of the users requiring protection'. Thus, if a company processes personal data through cookies, it must comply both with the GDPR and the ePrivacy Directive.

The ePrivacy Directive, before its amendment in 2009, did not contain consent as a requirement for the processing of data through cookies. Instead Article 5(3) permitted the usage of cookies on the condition that users are informed of the processing and have a right to refuse the placement and storage of cookies on their terminal equipment.[104] Thus, the original version of

[98] ibid Article 4(1).
[99] ibid.
[100] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 5–6.
[101] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (adopted on 20 June 2007) WP 136 14 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 17 April 2020.
[102] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 28.
[103] ePrivacy Directive Recitals 24 and 25.
[104] see also ibid Recital 25.

the ePrivacy Directive provided for an opt-out mechanism for cookie usage by websites.[105] The provision was later amended and the new wording explicitly required that subscribers or users give their prior consent to the use and storage of cookies on their device after having been informed of the purposes of the processing.[106] Thus, the legislators provided higher protection to users by making substantial amendments to this provision regarding the use of cookies[107] and changed the approach from an opt-out mechanism to an opt-in one.[108]

The amendment has, however, been criticised for not effectuating actual change in online business practices with respect to the use of cookies, especially in behavioural advertising.[109] Hence, the common practice of businesses, even after the significant change in the provision text, was to continue with opt-out methods instead of prior user consent. This is supported by the Cookie Sweep Combined Analysis report, which found that only 50% of the sites requested consent for the storage of cookies, while the other 50% merely stated that cookies would be used on the website.[110] Hence, websites' cookie practices do not seem to provide sufficient control to users, since half of them failed completely to comply with the legal requirement of prior opt-in consent. This poses a risk to data subject's fundamental rights to privacy and data protection.

It has been argued by Markou that the amendment improved only the information to be provided and displayed.[111] Hence, cookie information is not hidden anymore in the general privacy policies of businesses.[112] He also argued that the lack of change in practice is due to resistance and hostility from businesses, bad publicity and absence of enforcement actions by EU officials, national governments and data protection authorities.[113] Furthermore, the lack of consistent guidance by the WP29 and national regulators, such as, the ICO have 'muddled the waters',[114] as they took a stricter approach in their earlier guidance on Article 5(3), but became business friendlier in their later guidance.[115]

[105] Markou (n 88) 214, 221.
[106] see Citizens' Rights Directive Article 2(5).
[107] Opinion of AG Szpunar in *Planet49* (n 71) para 53.
[108] Markou (n 88) 214.
[109] see Markou (n 88).
[110] Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis' (n 83) 18.
[111] Markou (n 88) 226.
[112] ibid.
[113] ibid 227, 238–239.
[114] ibid 238.
[115] ibid 223–239, 240–241.

Another reason for the failure of Article 5(3) to bring effective change is due to implementations of the ePrivacy Directive on national level.[116] Fieldfisher compiled a table of national implementations in the 31 Member States belonging to the European Economic Area (hereafter the 'EEA') and identified whether or not the countries had implemented prior consent requirements as envisaged by the amendments to the provision.[117] The table, compiled in 2013 and amended in 2015, shows that only six EEA Member States incorporated prior consent into their national law. As a result, it is not strange that online businesses have continued the traditional practice of an opt-out system with respect to their cookie use. This issue can be rectified by the proposed ePrivacy Regulation, which does not require any national implementation of the law but will be directly applicable as its counterpart the GDPR.

Consequently, the burden will fall on national data protection authorities to take enforcement actions and not remain passive. Enforcement actions can provide incentive for companies to start making their cookie practices compliant. For example, the Dutch data protection authority published its investigations and findings on YD advertising agency's cookie practices for targeted advertisement and decided that an opt-out mechanism for cookies was in contrast to the national law requirements.[118] As a result of this publication many companies took the initiative to change their cookie policies, incorporate opt-in systems and remove 'cookie walls', which prevented users from accessing the website content unless they consented to the use of cookies.[119] Hence, this shows that enforcement actions can be effective in practice.

Additionally, a report by TRUSTe and Fieldfisher shows that from 2009-2013 'there was no meaningful enforcement of the EU's new cookie consent law'.[120] Consequently, many companies decided to halt their cookie compliance programs 'in order to prioritize more pressing compliance risks'.[121] Hence, this also supports the argument that active enforcement of cookie rules may be the key that triggers online businesses to change their practices and

[116] ibid 236, 241.
[117] Fieldfisher, 'Cookie "Consent" Rule: EEA Implementation' (Field Fisher Waterhouse) <https://res.cloudinary.com/fieldfisher/image/upload/v1574345727/PDF-Files/PDFs%20from%20old%20website/EU-Cookie-Consent-Tracking-Table-Fieldfisher-21-April-2015_fzwqve.pdf> accessed 18 February 2020.
[118] Ronald Leenes and Eleni Kosta, 'Taming the Cookie Monster with Dutch Law – A Tale of Regulatory Failure' (2015) 31 Computer Law & Security Review 317, 332 <http://www.sciencedirect.com/science/article/pii/S0267364915000059> accessed 26 February 2020.
[119] ibid.
[120] TRUSTe and Fieldfisher, 'EU Cookie Audits: Are You Ready?' 6 <https://iapp.org/resources/article/eu-cookie-audits-are-you-ready/> accessed 18 February 2020.
[121] ibid.

implement appropriate cookie consents. National data protection authorities have been more active in recent years in bringing enforcement actions under the GDPR.[122] Thus, it is hoped that they will expand this initiative to cookie compliance as well as soon as possible.

2.3 EXCEPTIONS TO COOKIE CONSENT

Article 5(3) of the ePrivacy Directive provides also for exemptions to the requirement of cookie consent. The provision excludes cookies from the consent requirement if they are used for i) 'technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network', or ii) 'as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'.[123] This is also emphasised in the Directive 2009/136/EC, which amended, inter alia, the ePrivacy Directive (hereafter the 'Citizens' Rights Directive'). Recital 66 provides that cookie consent and notice is not needed in 'those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user'.[124] Hence, the ePrivacy Directive recognises that websites do not need to obtain consent for all cookies, but only for the inessential ones, in other words, cookies which are not necessary for the provision of the website services.[125] These cookies might provide additional perks to the website operator if accepted by the user,[126] but the website can operate and provide its services even without them.

The WP29 considered, inter alia, that first party user-input session cookies,[127] authentication session cookies,[128] user centric security cookies,[129] multimedia player session cookies[130] and

[122] see for example 'GDPR Enforcement Tracker - List of GDPR Fines' <http://www.enforcementtracker.com> accessed 2 March 2020.
[123] see Article 2(5) of the Citizens' Rights Directive amending Article 5(3) of the ePrivacy Directive.
[124] ibid Recital 66.
[125] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 6.
[126] ibid.
[127] Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (n 80) 6. These cookies 'are typically used to keep track of the user's input when filling online forms over several pages, or as a shopping cart, to keep track of the items the user has selected by clicking on a button (e.g. "add to my shopping cart")'.
[128] ibid. 'Authentication cookies are used to identify the user once he has logged in (example: on an online banking website). These cookies are needed to allow users to authenticate themselves on successive visits to the website and gain access to authorized content, such as viewing their account balance, transactions, etc.'.
[129] ibid 7. These are 'cookies set for the specific task of increasing the security of the service that has been explicitly requested by the user. This is the case for example for cookies used to detect repeated failed login attempts on a website, or other similar mechanisms designed to protect the login system from abuses'.
[130] ibid. 'Multimedia player session cookies are used to store technical data needed to play back video or audio content, such as image quality, network link speed and buffering parameters'.

user interface customization cookies (such as, language preference cookies)[131] would be exempted from consent under Article 5(3).[132] On the other hand, tracking cookies, behavioural advertising and analytics cookies, especially third-party analytics cookies would always need user's consent.[133] The WP29, however, recognised that first-party cookies used for anonymized and aggregated statistical purposes 'are not likely to create a privacy risk'.[134] Thus, it recommended that legislators would add this as a third exemption in case the cookie consent provision will be addressed in the future.[135]

[131] ibid 8. 'User interface customization cookies are used to store a user's preference regarding a service across web pages and not linked to other persistent identifiers such as a username'.
[132] ibid 6–8.
[133] ibid 9–10.
[134] ibid 10.
[135] ibid 11.

3 Consent and Transparency

3.1 CONSENT

The notion of consent 'has roots in ancient Roman contract law', but since then it has extended its presence to other legal fields[136] and is quite a prominent tool in today's regime of privacy and data protection in the EU. Consent is recognised as a key element in data protection even on an international level.[137]

Consent has long been considered as a lawful ground in the EU's data protection framework based on which processing of personal data can become legitimate if correctly used.[138] For example, the Data Protection Directive Article 7(a) had already recognised in 1995 consent as one possible legal ground for processing personal data. This has now been replaced by Article 6(1)(a) of the GDPR, which continues to include consent as one of the six legal bases for processing personal data.[139] Furthermore, Article 8 of the Charter has cemented the prominence of consent in the EU's data protection regime,[140] by explicitly recognizing consent as a legal basis that legitimizes processing of personal data.

The requirements for a valid consent have not changed much over the course of EU's legislative history on data protection.[141] Conditions for a valid consent are currently laid down in Articles 4(11) and 7 of the GDPR. Consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a *statement or by a clear affirmative action*, signifies agreement to the processing of personal data relating to him or her'.[142] The definition of consent under the GDPR is thus very similar to the one in the

[136] Riikka Koulu, *Dispute Resolution and Technology: Revisiting the Justification of Conflict Management* (COMI 2016) 257, 259.
[137] Borgesius (n 40) 104; see also Organisation for Economic Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013) 14 <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> accessed 22 February 2020. The Collection Limitation Principle states that: 'There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.'; see also for example California Consumer Privacy Act 2018.
[138] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 2, 6.
[139] see Article 6(1)(a) of the GDPR.
[140] Carolan (n 46) 463.
[141] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 6.
[142] GDPR Article 4(11) emphasis added.

Data Protection Directive.[143] Consequently, the GDPR has not made any radical changes to the central elements of consent, but instead incorporated the WP29's recommendations.[144]

The concept of consent referred to in the ePrivacy Directive is defined in Article 2(f) and complemented by Recital 17. These provisions refer to the definition of consent in the Data Protection Directive, which has been replaced by the GDPR. Hence, the requirements for valid consent under the ePrivacy Directive are the same as under the GDPR. Consequently, the elements of freely given, specific, informed and unambiguous must also be present when website operators ask users for consent with respect to the use of cookies in order to constitute a valid consent.[145] The requirements of consent under the GDPR will also be applicable to the proposed ePrivacy Regulation.[146]

The reason why the conditions for consenting to processing of personal data are quite demanding is because the data subject by consenting to the processing of his or her personal data is at the same time 'waiving a fundamental right'.[147] Nevertheless, the data subject should be able to retain control over the use made of his or her personal data, which is why the element of control is also an aspect of valid consent. Furthermore, such control means also that the data subject should be able to withdraw his or her consent for future processing.[148] Hence, individual's right to self-determination and consent are inextricably linked as the 'autonomy of the data subject is both a pre-condition and a consequence of consent: it gives the data subject influence over the processing of data'.[149] As described above, the main requirements of a valid consent under the EU data protection framework are freely given, specific, informed and unambiguous indication. These requirements are analysed in detail below.

---

[143] Consent was defined under Article 2h of the Data Protection Directive as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' and Article 7 complemented the definition by stating that 'the data subject has unambiguously given his consent'.
[144] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (as last revised and adopted on 10 April 2018) WP 259 rev.01 3 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 26 February 2020.
[145] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 3.
[146] see Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2019) 12293/19 Article 4a(1).
[147] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 8.
[148] ibid 9.
[149] ibid.

3.2 FREELY GIVEN

The first element of a valid consent is the data subject's ability to exercise real choice regarding the processing of his or her personal data.[150] Real choice means that 'there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent'.[151] Coercion can be in the form of social, financial or psychological, etc.[152] If any of these factors are present then it should be interpreted that data subject has not been able to exercise freedom of choice.

Recital 42 of the GDPR has also clarified that consent is not to be considered freely given if the data subject is 'unable to refuse or withdraw consent without detriment'. This right is codified in Article 7(3) of the GDPR, which provides that it can be exercised 'at any time'. Withdrawing consent 'without detriment' means that data subjects must be able to take back their consent without any disadvantage or other negative consequences.[153] For example, controller cannot charge data subjects if they withdraw consent nor decrease the quality of its services.[154] These provisions reaffirm that data subjects should be able to change their minds with respect to consent, thus retaining some level of control all the time.[155] It has been said that 'the opportunity to change one's mind is itself a valuable right'.[156] Therefore, the right to revoke consent is also important to self-determination.

Furthermore, the condition of 'free will' means that consent cannot be considered as freely given in circumstances where there is an imbalance of power between the data subject and the controller, such as, employer vis-à-vis employee or public authority versus the data subject.[157] The WP29 has taken the view that whenever the controller has influence over the data subject, then it should be inferred that data subject is not able to exercise real choice.[158] Additionally, Article 7(4) and Recital 43 of the GDPR require that consent should not be part of the general

[150] ibid 12.
[151] ibid.
[152] Article 29 Data Protection Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)' (adopted on 15 February 2007) WP 131 8 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf> accessed 20 February 2020.
[153] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 10–11.
[154] ibid 21.
[155] ibid 5.
[156] PS Atiyah, *The Rise and Fall of Freedom of Contract* (Clarendon Press 2003) 756.
[157] GDPR Recital 43; Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 5–7.
[158] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 13.

terms and conditions of a service, but must be separate and the data subject must have a real choice in accepting or declining the processing of data that is not necessary for the provision of the service in question. Hence, the delivery of services cannot be conditional upon consent, where such processing of personal data is not necessary for carrying out the contract, otherwise the legislator will presume that consent was not given freely. Processing of personal data, which is necessary for the performance of a contract is a distinct legal basis from consent and these two legal bases 'cannot be merged and blurred'.[159]

With respect to the use of cookies the WP29 is of the opinion that real choice means that the 'user should have an opportunity to freely choose between the option to accept some or all cookies or to decline all or some cookies and to retain the possibility to change the cookie settings in the future'.[160] This coincides also with the requirements of specific consent, as cookies can be used for multiple purposes, from security purposes and language preferences to more invasive operations, such as, profiling and behavioural advertisement. Thus, cookie consent mechanisms should be designed in a way that offers granularity.

In conclusion, in order to fulfil the first condition of consent data subject must be able to exercise free will without any conditionality or 'inappropriate pressure or influence' or suffer any 'significant negative consequences' if consent is not given or it is later withdrawn.[161] Additionally, the data subject should be on an equal footing with the party requesting consent.

3.3 SPECIFIC

The second element of consent is that consent must be 'specific'. This element has also been elaborated in Article 6(1)(a) of the GDPR, which provides that consent must be given for 'one or more specific purposes'. Thus, the GDPR prohibits bundling of purposes together without any option to choose when asking consent from data subjects. Instead the data subject should be able to decide which purposes he or she accepts and which he or she declines.[162] Thus, Recital 32 states that if the processing contains multiple purposes, then 'consent should be

[159] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 8.
[160] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 5.
[161] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 5–7, 10.
[162] ibid 10.

given for all of them'.[163] However, it also states that once consent is provided for a purpose or purposes then it shall 'cover all processing activities carried out for the same purpose or purposes'. Thus, if the controller processes personal data for multiple purposes and consent is the appropriate basis, then there must be granularity, in other words, 'the separation of these purposes and obtaining consent for each purpose'.[164] For example, consent can cover the receipt of news on new products and their marketing, but it would not cover the transfer of personal data to third parties, as this would not be reasonably expected by the data subject.[165] Hence, this would require a distinct consent from the data subject, since the processing activities contain different purposes.[166] Furthermore, if the processing purposes for which consent was initially sought change over time, then the data subject must be informed of these changes and have a real choice of deciding whether to accept these new purposes, in order for the consent to continue to be specific.[167]

The principles of processing under Article 5 of the GDPR must also be taken into account when relying on consent as the legal basis. Consent does not provide freedom for controllers to ignore these data protection principles.[168] The principle of purpose limitation under Article 5(1)(b) of the GDPR provides that personal data must be processed for 'specified, explicit and legitimate purposes'. Identifying the purposes for which processing of personal data is needed acts as a 'safeguard against function creep'.[169] This phenomenon occurs when the processing purposes are blurred or gradually extended beyond what the data subject has initially consented to.[170] The consequences of function creep is that personal data may be used for purposes which are not reasonably expected by the data subject and additionally the data subject may end up losing control of his or her personal data.[171] Thus, this phenomenon contains an inherent risk to data subjects.[172] The legislators have sought to prevent this phenomenon of function creep by creating a buffer consisting of the requirements of specific consent and adherence to the principle of purpose limitation.[173]

---

[163] see also GDPR Recital 43 which states that controllers must 'allow separate consent to be given to different personal data processing operations'.
[164] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 10.
[165] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 18.
[166] ibid.
[167] ibid 19.
[168] ibid 7.
[169] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 11.
[170] ibid 12.
[171] ibid.
[172] ibid.
[173] ibid.

The CJEU addressed the meaning of 'specific' consent in the case of *Planet49* and stated that 'it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes'.[174] For example, in the case at hand, the court was of the opinion that it cannot be inferred that a user has given his or her consent to the use of cookies from the fact that he or she decides to participate in the lottery offered by the company Planet49 and thus clicks on the participation button.[175] The Advocate General (hereafter the 'AG') had similar reasonings and argued that the prerequisite for a freely given and informed consent is not only active behaviour, but that consent must also be separate from other action.[176] Hence, accordingly the AG contended that:

> The activity a user pursues on the internet (reading a webpage, participating in a lottery, watching a video, etc.) and the giving of consent cannot form part of the same act. In particular, from the perspective of the user, the giving of consent cannot appear to be of an ancillary nature to the participation in the lottery.[177]

The AG argued that clicking on the participation button once cannot cover '[t]wo expressions of intention… at the same time'.[178] Hence, according to the CJEU and the AG consent cannot be muddled with an act that expresses at the same time another intention or purpose.

In conclusion, the second element of consent, which is specific, requires that if the processing activities contain multiple purposes, then controller should seek consent for each separate purpose, rather than bundling them up. In other words, the element of granularity is important and must be present with respect to distinct purposes.[179] Furthermore, the act of consenting must be separate from other action, such as continuing on the website.

[174] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] OJ C 413, para 58.
[175] ibid para 59.
[176] Opinion of AG Szpunar in *Planet49* (n 71) para 66.
[177] ibid.
[178] ibid para 89.
[179] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 17, 19; Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 11.

3.4 INFORMED

The third element of valid consent is that consent must be 'informed'. The requirements that consent must be both specific and informed are related.[180] As a result, in order to fulfil the condition of 'specific consent', data subject must be informed about the intended purposes for which their personal data is being used.[181] Consequently, data subject's decision to accept the processing of his or her personal data must be based on appropriate information.[182] According to the WP29 'blanket consent without specifying the exact purpose of the processing is not acceptable'.[183] Additionally, consent can only apply to a set of processing activities, which have been clearly identified to the data subject and which the data subject can reasonably expect to be used in the processing context.[184] This condition requires also that the information about the processing of personal data must be clearly distinct from other information, such as, marketing material or the terms and conditions of the service.[185]

The WP29 has stated that this condition 'aims to ensure a degree of user control and transparency for the data subject'.[186] Though, the provision of information in itself will not automatically result in the data subject's consent, since another legal ground may be more appropriate or the data subject might simply reject, nevertheless, 'there must always be information before there can be consent'.[187] Thus, it is important that data subjects are provided with relevant information before their consent is obtained, so that they can make an informed decision.[188] Consequently, the requirements of prior information and informed consent are 'cumulative in nature'.[189] The information must also be easily accessible in order for data subjects to have real control over the processing of their personal data under consent.[190]

[180] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 17.
[181] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 12.
[182] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 3.
[183] ibid.
[184] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 17.
[185] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 11, 14.
[186] ibid 11.
[187] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 19.
[188] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 13.
[189] Clifford (n 48) 199.
[190] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 13.

The WP29 has instructed that cookie notices should be visible and communicated to the user prior to accepting the cookie settings.[191] It could, for example, be presented on the entry page or be behind a link, but the link must be displayed prominently on the webpage.[192] Furthermore, until the user has given his or her consent to the use of cookies, the website should keep displaying the relevant information.[193] With respect to cookies placed by an ad network agency that can sponsor many different website companies, the WP29 has recognised that asking for user's consent every time he or she visits a website partner of that ad network agency may be impractical.[194] The WP29 has therefore stated that 'the consent obtained to place the cookie and use the information to send targeting advertising would cover subsequent "readings" of the cookie that take place every time the user visits a website partner of the ad network provider which initially placed the cookie'.[195] Nevertheless, the WP29 recommends that the validity of such consent should be limited, for example to one year, so that consent is not given in perpetuity.[196] The ad network provider would then have to ask for new consent after the validity of the previous consent has elapsed.[197]

In conclusion, the requirement that consent must be informed means essentially that the data subject must be given prior and appropriate information about the processing purposes. In other words, companies are required to be transparent about their data processing operations. Nevertheless, though informed consent and the obligation to provide information are linked to each other they are still distinct obligations under the GDPR.[198] Controller's obligation to provide information to data subjects will be explored further below in subchapter 3.9.

3.5 UNAMBIGUOUS INDICATION

The fourth element of valid consent is 'unambiguous indication of the data subject's wishes', which must 'signify' data subject's agreement to the processing operations.[199] The provision

[191] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 3.
[192] ibid.
[193] ibid 4–5.
[194] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (adopted on 22 June 2010) WP 171 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 20 February 2020.
[195] ibid.
[196] ibid.
[197] ibid.
[198] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 19.
[199] GDPR Article 4(11).

clarifies also that the indication must be 'by a statement or by a clear affirmative action'.[200] Hence, making it clear that silence, or inaction,[201] or merely continuing with a service is not sufficient to constitute consent.[202] This is because silence and inaction have 'inherent ambiguity' in them and it is difficult to demonstrate that consent has been given through inaction or silence.[203] The WP29 has interpreted 'unambiguous' to mean that there must be '*no doubt* as to the data subject's intention to deliver consent'.[204]

GDPR prohibits also the use of pre-ticked opt-in boxes in Recital 32. Thus, valid consent under the Regulation 'must always be given through an active motion or declaration'.[205] This prohibition has also been confirmed by the CJEU in the *Planet49* case.[206] In its judgment the CJEU held that the wording 'given his or her consent' to the use of cookies requires action from the user when consenting.[207] This interpretation is also supported by the fact that both the Data Protection Directive and the GDPR require an 'indication' of the data subject's wishes in their definition of consent, which according to the court 'clearly points to active, rather than passive, behaviour'.[208] Furthermore, consent must also be 'unambiguous', which can only be fulfilled by active behaviour.[209] Thus, the court noted that a pre-ticked checkbox did not satisfy the notion of active behaviour by the user required under a valid consent.[210]

The court reasoned that the issues with a pre-ticked checkbox is that a) it could be possible that the website user has not read the notice regarding the checkbox, or b) not even noticed the checkbox, before submitting the form.[211] Hence, according to the court it is difficult to determine objectively whether the user has made an informed and positive decision to consent to the processing of his or her personal data by not removing the pre-ticked checkbox.[212] The court took also into account the fact that the legislators had in 2009 substantially modified

[200] ibid.
[201] ibid Recital 32.
[202] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 15–16.
[203] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 24.
[204] ibid 21 original emphasis.
[205] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 15–16.
[206] *Planet49* (n 174).
[207] see ibid para 49.
[208] ibid para 52.
[209] ibid para 54.
[210] ibid para 52.
[211] ibid para 55.
[212] ibid.

Article 5(3) of the ePrivacy Directive, by incorporating an explicit requirement to obtain consent before any cookies could be used or placed on a user's device.[213] Due to this amendment the court made the inference that 'henceforth user consent may no longer be presumed but must be the result of active behaviour on the part of the user'.[214]

Recital 66 of the Citizens' Rights Directive states that consent can be acquired through 'using the appropriate settings of a browser or other application', provided that the existing technology can generate consent mechanisms that will meet the criteria of valid consent.[215] This statement has garnered confusion in Member States over how to obtain cookie consent and has resulted in debates whether or not it is possible to imply consent from the default browser settings.[216] As the report from ENISA shows '[s]ome states have suggested existing browser settings would remain adequate, through the legal fiction that they convey "implicit consent". The majority view … is to require explicit, affirmative consent for each website'.[217]

The WP29 has made it clear that having browser settings in a mode where they accept the use of cookies by default, would not constitute a valid consent under Article 5(3) of the ePrivacy Directive.[218] It stated that the recital 'is not an exception to Article 5(3) but rather a reminder that, in this technological environment, consent can be given in different ways - where technically possible, effective and in accordance with the other relevant requirements for valid consent'.[219] Therefore, if browser settings have by default privacy protection on then it can be an effective tool in obtaining cookie consent.[220] It emphasised that active behaviour by the individual is the key to obtaining valid consent to cookies, hence consent can be obtained through browser settings provided that the website user has been 'fully informed and *actively* configured their browser'.[221] It goes without saying that nowadays, taking into consideration the spirit of the EU's data protection framework, which aspires to provide strong privacy

[213] see ibid para 56.
[214] ibid.
[215] Citizens' Rights Directive Recital 66.
[216] Clifford (n 48) 202.
[217] Claude Castelluccia and others, 'Privacy Considerations of Online Behavioural Tracking' (European Network and Information Security Agency (ENISA) 2012) Report/Study 16 <https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking> accessed 28 February 2020.
[218] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (n 194) 13–15.
[219] ibid 13.
[220] ibid 15.
[221] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 4 emphasis added.

protection for natural persons[222] and the privacy by design and by default principles introduced by the GDPR in Article 25, the browser settings of cookies should by default have the highest privacy settings on automatically.

The WP29 has also emphasised that it must be demonstrated that the positive action was taken as a result of user being well informed of the meaning of such action.[223] Hence, the appropriate information on the setting and use of cookies must be in close proximity to the button, link or box, through which the user indicates his or her consent to the cookies.[224] It must be clear to the user that the information and the active behaviour constitute the same package and the user must not confuse the information with other material, such as, advertisement.[225]

In conclusion, in order for consent to be 'unambiguous' there must be active behaviour on the part of the user. Pre-ticked boxes and other methods providing implicit consent, such as, default browser settings allowing cookies automatically, are no longer accepted under the GDPR.

3.6 OTHER ELEMENTS OF CONSENT

3.6.1 Timing

Processing of personal data cannot be commenced before data subject has provided his or her consent.[226] Thus, the timing of consent is crucial in order to make processing lawful.[227] As with its predecessor, the GDPR does not explicitly mention when exactly consent must be obtained. It can, however, be deduced from the language used in the legislation that the general rule is that consent must be obtained prior to commencing the processing in question.[228] For example Article 6(1)(a) of the GDPR states that processing is lawful only when the data subject 'has given consent'. This is further supported by the fact that if personal data is processed before consent is obtained, then the processing itself does not have any legal ground and is thus unlawful.[229]

[222] see for example GDPR Recitals 7 and 10.
[223] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 4.
[224] ibid.
[225] ibid.
[226] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 9.
[227] ibid.
[228] ibid 9, 30.
[229] ibid 30.

3.6.2 Evidence of consent

The WP29 recommended under the old legislation that controllers should be able to show evidence of given consent, so that consent can be verified in case any dispute arises, or consent is questioned by, inter alia, data subjects or regulatory authorities.[230] The GDPR incorporated this good practice into its framework and provides expressly in Article 7(1) that controllers shall be able to demonstrate that valid consent has been obtained. This is also confirmed in Recital 42, which stresses the importance of documenting consent.

3.7 EXPLICIT CONSENT

Companies and organisations processing special categories of personal data, such as, health data, political opinions and ethnic origin, which are considered sensitive, must obtain data subject's 'explicit consent' under Article 9(2)(a) of the GDPR. Thus, in these cases Article 6(1)(a) type of 'regular consent' is not sufficient. The difference between explicit consent and regular consent is, however, very fine. For example, the WP29 has recognised that a signed agreement or written statement of consent would demonstrate unambiguous consent.[231] Additionally, ticking a box is a commonly recognised way to show 'express, unambiguous consent' in both online[232] and offline environment. Both of these examples seem to, however, overlap with the concept of explicit consent. This is supported by the fact that the WP29 has asserted that explicit consent can be obtained through written statement and if needed including a signature.[233] Furthermore, it has stated that these methods would constitute express consent,[234] and that 'explicit consent' and 'express consent' as legal terms have the same meaning in law.[235] Yet, they are also using these methods as examples to show what constitutes unambiguous indication for the regular consent.

The WP29 has explained that explicit consent 'encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing'.[236] This seems to be very similar to regular consent, especially under the GDPR, since it also requires

[230] ibid 21, 25, 26.
[231] ibid 21.
[232] ibid 22.
[233] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 18.
[234] see Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 21, 22.
[235] ibid 25.
[236] ibid.

active behaviour by the data subject. The WP29 has further explained that the difference with explicit consent from the regular one is 'the way consent is expressed by the data subject'.[237] In other words, there must be an 'express statement of consent' by the data subject.[238] Nevertheless, they have used the term 'express statement' and 'express consent' in their earlier guidance when discussing unambiguous indication with respect to the regular consent under the Data Protection Directive.[239] This has not been addressed in their later guidance on consent under the GDPR, hence the WP29's interpretations are ambiguous.

Explicit consent cannot be inferred from data subject's actions, hence opt-out options would not suffice in meeting the conditions of explicit consent.[240] Thus, it is clear that explicit consent requires a positive action by the data subject, such as, completing an electronic form, sending an email,[241] or clicking on a button or an icon.[242] However, these seem like actions that would also be required when obtaining regular consent under the GDPR, since the WP29 has stated that 'data subject must have taken a deliberate action to consent to the particular processing', such as, writing a letter or typing an email.[243] A further step from this is to use two-stage verification in order to demonstrate explicit consent.[244]

Apart from the two-stage verification method, regular consent and explicit consent do not seem to differ that much from each other. This is especially the case since it is questionable whether even regular consent can be inferred from user's behaviour anymore under the GDPR, since it has provided a higher threshold than its predecessor[245] by requiring a clear and positive action. This is supported by the fact that the WP29 has stated with respect to the condition of unambiguous indication that it has to be 'obvious that the data subject has consented to the particular processing'.[246] This thesis argues that if regular consent must be 'obvious' under the GDPR, then it cannot really be inferred from any action. Hence, these two forms of consent are easily blurred, and it is doubtful whether explicit consent will in fact provide any better

[237] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 18.
[238] ibid 18.
[239] see Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 21, 22.
[240] ibid 25; Article 29 Data Protection Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)' (n 152) 9.
[241] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 18.
[242] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 26.
[243] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 16.
[244] ibid 19.
[245] ibid 18.
[246] ibid 15.

protection to sensitive personal data than regular consent, since the demonstrated methods for obtaining either consent are very similar. It is also debatable whether a consent can in fact be only unambiguous without being inherently also explicit. If this is not the case, then the difference between a regular and an explicit consent becomes illusory. It would be clearer if explicit consent would be defined as always needing for example two-stage verification, such as ticking a box and signing the form, whether electronically or manually.

3.8 TRANSPARENCY

The data protection regime in the EU and the guidelines adopted by the WP29 constantly emphasise on the data subject's right to be informed of the processing as discussed above. This is part of the transparency principle under the GDPR.[247] Though transparency has been a 'long established feature of the law of the EU',[248] it is a new explicit requirement in the data protection framework as a result of the GDPR[249] and is 'intrinsically linked to fairness and the new principle of accountability under the GDPR'.[250] In order for processing to be fair it must be transparent.[251] The accountability principle under the GDPR Article 5(2) obligates controllers to demonstrate compliance with the GDPR and hence processing operations must be transparent.[252] The GDPR holds no definition of transparency, but Recital 39 elaborates that it 'should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed'. Additionally, the same recital provides that data subjects 'should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing'.

Transparency is also an important feature with respect to consent as mentioned above. The precondition for obtaining an informed and specific consent is that data subject must be aware of what he or she is consenting to. Hence, for consent to be valid it must be based on prior

[247] GDPR Articles 5, 13 and 14; see for example Working Party on the Protection of Individuals with regard to the Processing of Personal data (n 24) 2.
[248] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 2.
[249] see GDPR Article 5(1)(a); cf Data Protection Directive Article 6(1)(a).
[250] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 2.
[251] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 9.
[252] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 2.

information. Transparency in itself does not make processing of personal data lawful, but it is 'a condition of being in control and for rendering the consent valid'.[253]

3.9 INFORMATION OBLIGATION

The European Commission has noted that since privacy policies are not always transparent enough, especially in the online environment, this raises the risk that website users are not sufficiently aware of their rights and therefore are unable to provide a valid consent.[254] The legislators have tried to tackle this by enhancing the transparency principle under the GDPR and improving the list of details in Articles 13 and 14 that companies must provide to data subjects when processing their personal data. Article 13 addresses situations when personal data is collected directly from the data subject, whilst Article 14 covers situations where personal data is collected from another source. Nevertheless, the information to be provided in either situation is similar, and they include, inter alia, controller's contact details, purposes of processing, legal basis, the recipients of personal data, whether data is transferred outside the EEA, the storage period and data subject's rights.

The GDPR has also emphasised in Article 12 that the information must be 'concise, transparent, intelligible and easily accessible form, using clear and plain language'. Thus, the Regulation seems to set a quite high threshold for the information obligation. Firstly, the information must be comprehensive in order to be transparent and informative to the data subjects, so that they are not 'taken by surprise at a later point about the ways in which their personal data has been used'.[255] In addition, the text must be written 'efficiently and succinctly in order to avoid information fatigue'.[256]

Secondly, the privacy or cookie notice must be written in intelligible, clear and understandable language, without any legal, technical or any other specialist jargon.[257] Furthermore, the text must be 'concrete and definitive; it should not be phrased in abstract or ambivalent terms or

[253] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 9.
[254] European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM (2010) 609 final.
[255] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 10.
[256] ibid para 8.
[257] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 20; Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 13.

leave room for different interpretations'.[258] In terms of consent, it can only be informed if the data subject understands the consequences for consenting and withholding consent.[259] A rule of thumb for writing a privacy or cookie notice is that a 'regular/average user should be able to understand it'.[260]

Thirdly, it must be clear to the data subject where he or she can find the information.[261] Thus, it is 'not enough for information to be "available" somewhere'.[262] Even the CJEU addressed this in 2004 in joined cases, where it held that consent was not validly given when an employment contract merely referred to another contract that contained the conditions to which consent was given.[263] The WP29 has emphasised that the 'information must be clearly visible'[264] and distinct from any other information, such as, the general terms of use.[265] Information can be provided by different means, though Article 12(1) explicitly mentions 'in writing', hence making it the default position.[266] Other methods explicitly recognised by the provision include electronically and orally.

The first two requirements provide a difficult hurdle for controllers to overcome, since in order for the privacy or cookie notice to meet the standard envisioned by the GDPR, it must be both sufficiently detailed in order to be comprehensive but also clear and understandable. This can be difficult, especially with respect to cookies, since explaining the cookie technology in a clear and intelligible manner can be difficult. The WP29 has recognised this conflict in the GDPR and stated that:

> There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the

[258] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 12.
[259] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 20.
[260] ibid.
[261] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 11.
[262] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 20.
[263] Joined Cases C-397/01 to C-403/01 *Bernhard Pfeiffer and Others v Deutsches Rotes Kreuz, Kreisverband Waldshut eV* [2004] ECR I-08835, para 75-86.
[264] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (n 38) 20.
[265] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 8.
[266] ibid para 17.

> GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible.[267]

The WP29 recommends websites to use layered privacy notices 'in order to avoid information fatigue', as this method 'can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read'.[268] Nevertheless, the WP29 also recognises that the whole information notice must be available to data subjects 'in one single place' or as 'one complete document' in case a data subject wants to check the privacy notice in its entirety.[269]

3.10 CONCLUSION

This chapter has outlined the components of consent and the principle of transparency under the GDPR. As has been discussed above, in order for consent to be valid it must be freely given, informed, specific and unambiguous. This thesis argues that consent is in itself a difficult threshold to overcome, since it constitutes so many elements. Each component must be present before consent is considered valid under the GDPR. Consent can arguably be an effective tool in providing control to data subjects if correctly used, because it enables data subjects to exercise the right to self-determination. In contrast, if consent does not meet its requirements of valid consent imposed by the data protection law, then data subjects will not have effective control over their personal data. Additionally, companies will face serious compliance risks if they process personal data under an invalid consent as they will not have a valid legal basis for their processing activity which has relied on consent.

It can also be argued that consent is not an effective tool in the online environment in providing control to users, because there will always be some level of imbalance of power between the website operators and internet users, due to the substantial use of the internet in the modern world and its importance in people's lives. Additionally, it could be argued that there is also, to a certain extent, social pressure or influence, especially with respect to social media sites. For example, as many people use Instagram, Facebook, Zoom and LinkedIn, an individual can feel secluded from his or her friends and peers if he or she does not join these communities as

[267] ibid para 34.
[268] ibid para 35.
[269] ibid para 17.

well irrespective of the privacy risks.[270] Thus, it can be argued that consent is not the appropriate legal basis for processing personal data through cookies, since it lacks the element of free will.

Furthermore, the information obligation contains some conflicting features as the GDPR requires the information to be both clear and easily understandable but also comprehensive. Arguably, one way to deal with this tension is to use layered information as recommended by the WP29. The question is whether individuals will actually read the information provided to them before consenting. This issue is further explored in the next chapter. Nevertheless, this is a difficult hurdle, as evidenced by the Cookie Sweep Combined Analysis report. The WP29 inspected in this report the cookie notifications of 404 websites in more detail and drew the conclusion that 43% did not provide sufficient information to enable the user to make an informed decision regarding the use of cookies.[271] It did not, however, go into detail as to what was lacking in these cookie notices. Since, the information obligation requirements are conflicting it is questionable whether companies will be able to meet the GDPR standard. Failure to provide sufficiently detailed, yet, clear and understandable information means that data subjects will not be able to make an informed decision regarding the use and disclosure of their personal data. Hence, consent and notice are not an effective tool in providing control and protection to individuals in the context of personal data processed through internet cookies.

This thesis has also criticised the WP29's ambiguous guidance concerning 'regular consent' and 'explicit consent'. The lack of clear explanation between the differences of these two forms of consent can result in controllers using the explicit consent form as a 'just in case' method. Alternatively, they might not meet the threshold of regular consent, if they cannot see the difference between regular and explicit consent requirements. Hence, better clarification is in order when distinguishing these two consent forms so that they can be used accurately.

---

[270] see for example Kari Paul, 'Worried about Zoom's Privacy Problems? A Guide to Your Video-Conferencing Options' *The Guardian* (9 April 2020) <https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives> accessed 4 May 2020; Rae Hodge, 'Zoom Security Issues: Zoom Could Be Vulnerable to Foreign Surveillance, Intel Report Says' (*CNET,* 8 May 2020) <https://www.cnet.com/news/zoom-security-issues-zoom-could-be-vulnerable-to-foreign-surveillance-intel-report-says/> accessed 4 May 2020; 'Facebook to Pay $5bn to Settle Privacy Concerns' *BBC News* (24 July 2019) <https://www.bbc.com/news/business-49099364> accessed 4 May 2020; Vivian Ho, 'Facebook's Privacy Problems: A Roundup' *The Guardian* (15 December 2018) <https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup> accessed 4 May 2020.

[271] Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis' (n 83) 18.

4 Effectiveness of Cookie Consents and Notices

4.1 PROBLEMS WITH COOKIE CONSENT

As has been recognised above, consent is an established legal basis making data processing lawful. There is, however, criticism on consent and whether it is the appropriate tool in privacy and data protection in the online environment. It has, for example, been criticised that the European lawmakers have been unwise in 'introducing consent as a legal ground in the sphere of human rights'.[272] This criticism can be applied to privacy and data protection, since these are fundamental human rights in the EU, as established in the introductory chapter of this thesis.

In the modern times personal data is quite essential to most online services in order for them to function.[273] As a result, internet users may find themselves exhausted by having to reply to a number of consent requests left and right on a daily basis.[274] This 'click fatigue' can in turn result in blindly accepting cookies as users will not be bothered to read the cookie information, in which case there is no longer an effective and valid consent.[275] This subchapter explores the criticism by academics and discusses whether consent is an effective tool for lawmakers to cling onto in the context of cookies. It should be noted that some of the discussion will overlap with the debate on the effectiveness of cookie notices, which will be further explored in subchapter 4.2. This is because, as has been mentioned previously, the obligation to provide information is also essential in the context of consent, since valid consent means that the user has been informed.

4.1.1 Economic Theory and Behavioural Economics

Professor Borgesius has recognised that today's lawmakers in privacy and data protection give much importance to consent.[276] He has, however, claimed that 'behavioral studies cast doubt on this approach's effectiveness, as people tend to agree with almost any request they see on their screens'.[277] Borgesius discusses the issues with consent in practice with respect to behavioural targeting using economic theory and behavioural economics. Behavioural

[272] Paul de Hert, 'Reply: The Use of Labour Law to Regulate Employer Profiling: Making Data Protection Relevant Again' to Nils Leopold and Martin Meints, 'Profiling in Employment Situations (Fraud)' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) 232.
[273] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 17.
[274] ibid.
[275] ibid.
[276] Borgesius (n 40) 103.
[277] ibid.

economics utilizes psychology and behavioural studies when analysing people's decision making process in economics.[278] His analysis can also be applied to cookie usage in general, since behavioural advertising is generally carried out through cookies.[279] In Borgesius' opinion, accepting cookies is similar to 'entering a market transaction with a company'.[280] In this transaction the effect of consent is, however, reduced by 'information asymmetries' and 'transaction costs'.[281]

Information asymmetries arise due to lack of users' knowledge about how companies use their data, which results in a deficient informed consent.[282] Other scholars have also recognised information asymmetry as a reason for the failure of consent.[283] Information asymmetry seems to continue to be a problem even after the GDPR, which aimed to tackle this issue through the requirement of transparency, so that companies are obligated to inform users about their data processing operations. The Special Eurobarometer on the GDPR, conducted in March 2019, shows that only 22% of the respondents using the internet replied that they feel like they are always informed about the data processing operations.[284] The survey also shows that in most countries there has been more decrease in awareness than increase compared to 2015.[285]

Borgesius argues that legislators have been unsuccessful in tackling information asymmetry due to the accompanying transaction costs.[286] According to this theory, users rarely read privacy policies because they tend to be heavy, ambiguous and not reader friendly, hence it would be too time consuming for users to actually familiarise themselves with these policies.[287] This argument is supported by a research conducted by McDonald and Cranor in the US that discovered that if internet users would read the complete online privacy policies of all new

[278] ibid 105; Richard Partington, 'What Is Behavioural Economics?' *The Guardian* (9 October 2017) <https://www.theguardian.com/world/2017/oct/09/what-is-behavioural-economics-richard-thaler-nobel-prize> accessed 8 May 2020.
[279] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (n 194) 4, 6.
[280] Borgesius (n 40) 104.
[281] ibid.
[282] ibid.
[283] see for example Shara Monteleone, 'Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation' (2015) 43 Syracuse Journal of International Law and Commerce 69, 88 <https://heinonline.org/HOL/P?h=hein.journals/sjilc43&i=71> accessed 25 February 2020.
[284] European Commission, 'Special Eurobarometer 487a: The General Data Protection Regulation, Full Report' (2019) QB13 <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222> accessed 4 April 2020.
[285] ibid 44.
[286] Borgesius (n 40) 104.
[287] ibid.

websites that they visit in a year, then this would take around 40 minutes per day and cost $781 billion to the nation.[288] It has been stated that '[i]t would be a full-time job to protect your privacy in a notice and consent mode', especially since the average user's limited time is already divided between work, family and hobbies.[289]

Furthermore, according to Borgesius, people are also influenced by biases, such as, the status quo bias, which is 'the tendency to stick with default options', and the present bias, which is 'the tendency to choose immediate gratification and disregard future costs or disadvantages'.[290] Hence, according to the status quo bias companies are likely to obtain more consents in an opt-out system, because people are not inclined to change the default option.[291] The present bias, on the other hand, shows that if companies use cookie walls, meaning that access to the website is conditional upon accepting the use of cookies, then people are more willing to click on the accept button, without concerning them with its consequences, because they want to access the website and its services.[292] Thus, as has been said by professor Solove 'privacy is an issue of long-term information management, while most decisions to consent to the collection, use, or disclosure of data are tied to a short-term benefit'.[293] This issue could be partly reduced by rules which prohibit cookie walls. However, as will be seen in subchapter 6.1 of this thesis, the debate regarding cookie walls is still ongoing under the proposed ePrivacy Regulation.

Borgesius has rightly claimed that the effectiveness of consent in cookie usage is diminished if websites are allowed to use cookie walls, as this provides a 'take it or leave it' type of situation.[294] This will inevitably impose some influence on the individual's choice, which can be especially powerful if the user cannot attain same or similar services from another website. As discussed above, consent is not free if data subject is influenced in his or her choice. Hence, it is argued that there can never be valid consent when using cookie walls, as the user is essentially forced to accept the cookies if he or she wants to access the website services.

---

[288] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 ISJLP 543, 544, 563, 564 <https://heinonline.org/HOL/P?h=hein.journals/isjlpsoc4&i=563> accessed 20 March 2020.
[289] Kate Fazzini, 'Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but so Far It's Mostly Created Frustration for Users, Companies, and Regulators' (*CNBC*, 5 May 2019) <https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html> accessed 6 May 2020.
[290] Borgesius (n 40) 105.
[291] ibid.
[292] ibid.
[293] Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880, 1891 <https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/> accessed 24 February 2020.
[294] Borgesius (n 40) 105.

4.1.2 Cognitive and Structural Problems

Solove has also recognised that privacy and data protection laws aim 'to provide people with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information'.[295] He calls this approach 'privacy self-management', which 'takes refuge in consent'.[296] In his opinion, there are two issues with privacy self-management, which makes it unsuccessful in conferring to individuals 'meaningful control over their data' and these are i) cognitive problems and ii) structural problems.[297]

Cognitive problems explain why people are unable to make informed and rational choices when it comes to weighing the costs and benefits of allowing the use of their personal data.[298] The first related problem to the cognitive concern is the issue of informing individuals about the use made of their data so as to enable them to choose whether or not to consent.[299] Solove, however, argues that there is an inherent problem with notices, because 'making it simple and easy to understand conflicts with fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful'.[300] Hence, it seems to be almost impossible to make a privacy notice clear, short and comprehensive all at the same time as required under the GDPR.[301] It could arguably be overcome by the use of granular information, though Solove has argued that 'additional granularity adds complexity and create risks of confusion'.[302]

The second related problem under the cognitive issue is that people's decision making is skewed and that they do not have the 'expertise to adequately assess the consequences of agreeing to certain present uses or disclosures of their data', even if they would constantly read privacy policies.[303] This is due to people's 'bounded rationality' in which individuals 'struggle to apply their knowledge to complex situations',[304] and instead they 'often rely on rules of

[295] Solove (n 293) 1880.
[296] ibid.
[297] ibid.
[298] ibid 1880, 1881.
[299] ibid 1883.
[300] ibid 1885.
[301] see GDPR Article 12(1).
[302] Solove (n 293) 1885.
[303] ibid 1886.
[304] ibid 1887.

thumb or heuristics'.[305] Another factor affecting individual's decision-making is 'availability heuristics', which means that in people's minds, dangers which they have not encountered before are not seen as risky as dangers which they are familiar with.[306] Solove argues that the reason why individual's decision making is skewed and easily affected by these and other factors is because 'privacy is so complex, contextual, and difficult to conceptualize'.[307]

This thesis agrees with Solove's above statement that, since privacy and data protection are quite abstract, it might be difficult for data subjects to understand the risks entailing in recklessly disclosing their personal data, especially in the online environment. Furthermore, the fact that users cannot check from one place all the data that is available about them on the internet makes this an invisible threat. If individuals could check their 'data account' to see the total amounts of data and the type of personal data that is available to companies and governments, they might become more cautious in exchanging their personal data for 'free services' online. Data subjects do have the right to access their data and get a copy of it under Article 15 of the GDPR. However, since people's personal data is processed by many different website operators, data subjects would have to request access from all of them, in order to get a comprehensive picture of all their personal data moving around in the internet. Thus, there is no one data account for a user's personal data. The allure of 'free services' and the inclusiveness offered by the internet community is very powerful, which is why people are willing to give away their personal data relatively easily without thinking too much about it.

Moving on to structural problems, Solove claims that even if people are 'fully informed and rational' they will still be burdened by structural problems, which 'involve impediments to one's ability to adequately asses the costs and benefits of consenting to various forms of collection, use and disclosure of personal data'.[308] In terms of structural problems, Solove recognises first the 'problem of scale'.[309] This refers to the problem that it is impossible for individuals to control and monitor all entities processing their personal data, due to the large scale, regardless if all companies constructed intelligible privacy management tools for them.[310] This is because people lack time and resources.[311] Consenting to cookies on every

[305] Borgesius (n 40) 105.
[306] Solove (n 293) 1887.
[307] ibid 1888.
[308] ibid.
[309] ibid.
[310] ibid.
[311] ibid 1888, 1889.

single website that a user visits during a day can be exhaustive as a data subject can visit dozens of websites in a day.[312] Furthermore, as Solove contends, companies tend to update their privacy policies, which means that data subjects would have to revisit them,[313] and make a new informed decision about whether or not to let the company process their personal data. It could, however, be counterargued that companies probably do not update their privacy policies that frequently (maybe once a year), unless their processing operations undergo some significant changes. Nevertheless, this can still become burdensome for the user considering all the privacy policies he or she would have to revisit if all the websites he or she has visited in a year annually update their privacy policies.

The second issue under structural problems raised by Solove is the 'aggregation effect', whereby different portions of data, which have been given in isolation, are combined and may thus reveal new information about the person in question.[314] It may be difficult for data subjects to understand and asses the risks and benefits of aggregated data at the time of data collection, when consent is usually asked, as the consequences of aggregated data, whether beneficial or harmful, tend to reveal itself at a later time.[315]

The issue with aggregation effect is also applicable to cookies, especially third party cookies placed by ad network agencies. This is because data subjects may give consent to various websites to use third party advertising cookies, without realising that some or many websites might use the same ad network agency. This means that the same ad network will track the user's behaviour on the different websites that it has partnered with and collect vast amount of information, which it can combine in order to create a detailed profile of the user.[316] A data subject may consider that consenting to cookies on individual webpages is very innocent as he or she drops individual pieces of data in different contexts. Nevertheless, combined these innocuous data can together reveal sensitive data. This is supported by Dr. Betkier, who has stated that '[p]eople may be unable to make a rational trade-off between the privacy risk and economic benefit, even if they have a choice and have read and understood the privacy policy. One reason for this is the problem of the complexity of choice due to data aggregation'.[317]

[312] ibid 1888.
[313] ibid 1889.
[314] ibid 1889, 1890.
[315] ibid 1890.
[316] Markou (n 88) 216.
[317] Betkier (n 40) 35.

Hence, he argues that consent 'may not be the appropriate authorisation method for the online environment'.[318]

Thirdly, Solove recognises the 'problem of assessing harm' as part of structural problems and stated that 'Harm from privacy violations can develop gradually over time, but decisions about privacy must be made individually, in isolation, and far in advance.'[319] Furthermore, individuals tend to 'favor immediate benefits even when there may be future detriments'.[320]

4.1.3 Criticism of Opt-in Consent Systems

The opt-in consent system has been criticised as it may be 'unnecessarily costly and impede socially beneficial uses'.[321] This opt-in and prior notice system has also generated criticism from Clifford, who has stated that: 'The more common cookie notices become, the more mundane, easily dismissed and ineffective the obligation to consent is rendered.'[322] In his opinion, EU lawmakers should focus more on privacy by design rather than the controversial concept of consent, as data subjects are best protected when applications and software are inherently built with privacy protective features.[323] He has stated that 'the future of protection lies with laws regulating manufacturing standards and the concept of privacy by design'.[324] This is also supported by Hildebrandt and Tielemans, who have stated that: 'This would incentivize technological innovation with regard to built-in data protection, because once such technology is state of the art it becomes the legal standard.'[325] The GDPR has incorporated privacy by design requirement, but it remains to be seen how effective this will be. Mitchell has also expressed his doubts about whether an opt-in consent model will do anything to protect users better than an opt-out system. He has rightly claimed that:

> While this approach certainly solves the dilemma of reasonable data privacy expectations, it does not address what I believe is the fundamental problem associated

[318] ibid.
[319] Solove (n 293) 1891.
[320] ibid.
[321] ibid 1899.
[322] Clifford (n 48) 204.
[323] ibid 209.
[324] ibid.
[325] Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law & Security Review 509, 516 <http://www.sciencedirect.com/science/article/pii/S0267364913001313> accessed 28 February 2020.

> with modern internet use: in order to use the internet for any purpose, individuals must sacrifice their right to data privacy in some measure. Such conditional use always puts the user at a substantial disadvantage. The bargaining leverage websites enjoy in this regard borders on coercion, especially when considering the modern need of internet use and the substantial sacrifice associated with private data access.[326]

Carolan has also noted that 'there is little, if any, qualitative difference between default settings of which the user is unaware and the default settings to which a user is invited to "click" their unthinking approval'.[327] Jones and Tahir have argued that another issue with an opt-in consent, as a tool for enabling the use of cookies, is the question of how website operators are going to 'identify and keep track of users who have consented to the use of cookies'.[328] This thesis argues that keeping track of users who have consented should be easier, than keeping track of those who have refused cookies, since website operators need to store and document the consent, as required under the GDPR Article 7(1). But, if user refuses the storage of cookies on his or her device, including the cookie containing an ID number, then website operators will not have any means of identifying (except maybe with an IP address[329]) when the same user returns or when the same user visits different websites backed up by the same advertisement network. This means that the user who has refused cookies would have to do so every time he or she visits the website, which could also result in click fatigue.

Despite all the criticism, there are scholars who have also acknowledged the value of an opt-in model. Monteleone, for example, recognises the importance of an opt-in system due to the status quo bias, hence she states that 'this highlights the relevance of default privacy settings for the privacy online'.[330] Tene and Polonetsky have also acknowledged the value of having

---

[326] Ian D Mitchell, 'Third-Party Tracking Cookies and Data Privacy' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2058326 9 <https://papers.ssrn.com/abstract=2058326> accessed 28 February 2020.
[327] Carolan (n 46) 470.
[328] Richard Jones and Dalal Tahri, 'An Overview of EU Data Protection Rules on Use of Data Collected Online' (2011) 27 Computer Law & Security Review 630, 635 <https://linkinghub.elsevier.com/retrieve/pii/S0267364911001488> accessed 25 March 2020.
[329] see Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] OJ C 475. The CJEU held that dynamic IP addresses can qualify as personal data in circumstance where the website operator has the legal means to identify the individual by combining the IP address with the information that the internet service providers ('ISPs') have on that person. Thus, individuals can be indirectly identified from the IP address. As a result, IP addresses can only be processed with the data subject's consent or based on the controller's legitimate interest, for example for security purposes.
[330] Monteleone (n 283) 108.

distinct opt-in and opt-out models.[331] They argue that those activities, which are socially acceptable should benefit from 'implicit' rather than 'explicit' consent.[332] In their view:

> Some activities are value creating, socially desirable, and minimally intrusive; they should be permitted to exist as default options. Other activities are privacy intrusive, socially menacing, and may inflict real harm on users; they should be prohibited absent users' informed, explicit, opt-in consent.[333]

It is, however, questionable whether an opt-in system actually effectuates a better consent, since arguably data subjects might just automatically click on the accept button, without really thinking about it as they are impatient to get to the website. As Carolan has stated 'that active step can itself become the effective default option'.[334]

4.1.4 Other Criticism and Alternative Methods

Mantelero has also criticised the traditional 'notice and consent' model in the modern age of Big Data.[335] In his view, this traditional model does not work in situations of complex data processing operations, as data subjects do not have the capability to comprehend the data processing and its purposes in these cases and are thus unable to exercise self-determination and make informed decisions.[336] Hence, he argues that in these types of complex situations 'the decision about data processing cannot be left to users, but at the same time user's rights to oppose to data processing and not to have personal data collected … should be preserved'.[337] In these cases, he suggests that policymakers should adopt a new paradigm constituting of data protection impact assessments, which are 'based on the model of risk analysis and evaluate *ex ante* the future impact that a specific services or product could have on privacy or data protection'.[338] The assessment should be carried out by qualified third parties and subject to the supervision by data protection authorities.[339]

[331] Tene and Polenetsky (n 49) 334.
[332] ibid 338.
[333] ibid 341.
[334] Carolan (n 46) 470.
[335] Mantelero (n 40) 644–645.
[336] ibid 659.
[337] ibid 655.
[338] ibid 656 original emphasis.
[339] ibid 656, 657.

In his opinion, data protection authorities have better knowledge of the technological complexities raised by data processing and are in a better position to 'evaluate the risks associated to data processing and can adopt legal remedies to tackle them'.[340] The company should inform the data subjects of the results of the data protection impact assessment and provide them the opportunity to opt-out from the data processing.[341] Thus, Mantelero recommends a model that combines both a data protection impact assessment and opt-out system.[342] In his opinion:

> From the user's point of view, on one hand the assessment conducted by the data protection authorities gives a guarantee of an effective evaluation of the risks related to data processing and, on the other hand, the opt-out allows users to receive information about data processing and to decide if they do not want to be part of the data collection.[343]

The GDPR has introduced data protection assessment, which should be conducted in certain situations, such as, in automatic profiling.[344] Thus, the legislators have recognised the importance of pre-emptive steps combined with an opt-in approach. This seems to provide a comprehensive protection to data subjects even in the online environment. However, under the GDPR data protection assessment is conducted by the company itself and it does not need to be public.[345] Therefore, this assessment under the GDPR is not as transparent as it could be.

Mantelero's idea is in theory good, but in practice it can be quite difficult to implement, especially if data protection authorities have to take the initiative to supervise all data protection projects of all companies under their jurisdiction. This would be very cumbersome to put into effect in practice and overload the data protection authorities even more, who are already understaffed since the GDPR came into force.[346] Nevertheless, Article 36 of the GDPR has recognised that the controller must turn to a data protection authority for prior consultation in case the data protection impact assessment 'indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk'. Hence, in certain

[340] ibid 653.
[341] ibid 657.
[342] ibid 655.
[343] ibid 658.
[344] see GDPR Article 35(3)(a).
[345] see ibid Article 35.
[346] Fazzini (n 289).

circumstances data protection authorities do have a more active role when it comes to supervising data protection impact assessments.

Tene and Polonetsky have also recognised the 'increasing complexity of the online information ecosystem'.[347] They have argued that requiring users to decide whether or not to consent to divulge their data in this complex environment is 'tantamount to imposing the burden of health care decisions on patients instead of doctors'.[348] The authors have also argued that instead of shifting the burden to users, policymakers 'should focus on the limits of online behavioral tracking practices by considering which activities are socially acceptable and spelling out default norms accordingly'.[349] The authors argue that consent and transparency mechanisms 'are inherently skewed' and therefore these mechanisms are applied inconsistently.[350] Hence, they argue that instead of having notice and consent at the centre, 'the focal point for privacy should shift from users to policymakers or self-regulatory leaders, to determine the contours of accepted practices, and businesses, to handle information fairly and responsibly'.[351] This shift of privacy burden from users to companies 'will have the effect of making online privacy a matter of corporate governance'.[352] This is what the GDPR has attempted to do, as it places the burden on companies to process personal data fairly and transparently and for them to be held accountable if they fail to meet their obligations under the Regulation.

Providing a valid consent in the online environment is further complicated by the fact that there is a limited choice of service providers that provide the same services, especially with respect to the popular ones, for example, Facebook and Google.[353] Data portability is now possible under Article 20 of the GDPR, which makes switching service providers easier as data subjects have the right to have the old service provider transfer all their personal data to the new service provider. Nevertheless, it has been argued by Dr. Betkier that 'a strong "network effect" exists caused by the overwhelming majority of users subscribed to the "main" service providers',[354] which deters many from changing service providers. Thus, as users may be influenced by these factors when giving consent it is not really freely given.[355]

[347] Tene and Polenetsky (n 49) 285.
[348] ibid.
[349] ibid.
[350] ibid 287.
[351] ibid 336.
[352] ibid 348.
[353] Marcin Betkier, *Privacy Online, Law and the Effective Regulation of Online Services* (Intersentia 2019) 35.
[354] ibid.
[355] ibid.

Despite all the criticism surrounding consent in the online environment, according to Markou 'privacy is so intrinsically connected with consent that the latter could never be abandoned as a principal tool of privacy protection'.[356] He also argues that since the prior consent mechanism in the amended Article 5(3) of the Privacy Directive has 'never consistently been implemented by (major) online businesses', there is not sufficient evidence to state that consent does not work with respect to cookies.[357] It has also been stated by Koulu that 'consent has proven … to be exceptionally durable'.[358] Tene and Polonetsky have also acknowledged the importance of consent in privacy law, though they criticise it for being an 'elusive concept', a 'wild card' and 'seldom truly voluntary', since it is encumbered by power imbalance, such as, consumers against big corporations.[359] Nevertheless, they agree that 'consent cannot be entirely done away with, since conceptions of privacy typically incorporate control as a key component, or indeed describe privacy as a form of control over information'.[360] Therefore, consent, which is 'the manifestation of individual control – is inextricably tied to privacy'.[361] Furthermore, they argue that the absence of consent in privacy law would make it 'overly rigid and paternalistic'.[362]

As the notion of consent is so entrenched in the EU's data protection framework and especially with respect to cookies, it is unlikely that the EU legislators will abandon consent easily and in the near future as a tool for the lawful use of cookies. This can be seen from the proposed ePrivacy Regulation, as none of its previous drafts have even suggested an alternative legal basis for the use of cookies, but instead kept riding on the traditional consent practices as a habit. There is, however, a change of wind coming with the newest revised version by the Croatian Presidency adopted on 21 February 2020, who has taken the step to include legitimate interest as an alternative legal basis for cookies. This is further discussed below in subchapter 6.2.

It has been stated by Lindqvist that 'some feel that data protection legislation stiffens innovation altogether',[363] although the author has not explained who these people are. It can, however, be assumed that this includes at least entrepreneurs and other people in the business

[356] Markou (n 88) 241.
[357] ibid 242.
[358] Koulu (n 136) 257.
[359] Tene and Polenetsky (n 49) 338.
[360] ibid.
[361] ibid.
[362] ibid.
[363] Lindqvist (n 46) 2.

industry, who are more concerned with profits and economic growth, where innovation is a big part of the scenario. Nevertheless, instead of resulting in an impasse of innovation, data protection legislation should be seen as a challenge to think outside the box and invent technologies with strong built-in privacy protection. This in turn would result in privacy protective technologies to become state of the art as highlighted above by Hildebrandt and Tielemans.[364] Thus, as suggested by Hildebrandt '[w]hat we need is an intelligent interplay between technological design and legal regulation, with a keen eye to market forces and business models as they will fit in with such design and regulation'.[365]

4.2 PROBLEMS WITH COOKIE NOTICES

Transparency, though an important principle, is also surrounded by criticism. Koivisto has stated that 'we live in the era of transparency', everything should be transparent from state governance to society itself, thus transparency is 'the New Norm' of the modern civilisation.[366] The author has criticised the concept for being ambiguous and lacking a uniform definition.[367] Maybe this is the reason why the EU legislators did not provide a definition of transparency in the GDPR.

It could be argued that the reason why transparency is important in modern society is because as a notion 'its promise of letting us see and understand is seductive'.[368] Arguably, if people understand how those in power exercise this privilege, they can be held more easily accountable and thus ensure that power is not abused. Therefore, as Koivisto has stated the 'idea is that transparency makes power visible and, as such, controllable'.[369] Nevertheless, though transparency seems to be an important feature in today's global governance, as it has an 'inherent capability of exposing the "truth"',[370] it might not necessarily be efficient. This is supported by Koivisto, who has argued that just because we see, does not mean we always understand.[371] She has also criticised that 'transparency neither addresses the beholder's

[364] see Hildebrandt and Tielemans (n 325) 516.
[365] Mireille Hildebrandt, 'Profiling and the Identity of the European Citizen' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) 325.
[366] Koivisto (n 46) 1.
[367] ibid 2.
[368] ibid 10.
[369] Ida Koivisto, 'The IMF and the Transparency Turn' (2016) 25 Minnesota Journal of International Law 381, 383 <https://heinonline.org/HOL/P?h=hein.journals/mjgt25&i=393> accessed 17 March 2020.
[370] ibid 386.
[371] Koivisto (n 46) 10.

capacity to interpret what she sees nor the target's capacity to manipulate its representation'.[372] Furthermore, Koivisto is of the opinion that 'transparency practices do not necessarily check power, but can relocate and even produce it', and therefore according to her 'transparency is a contradictory concept which carries the possibility of non-disclosure in itself'.[373]

Privacy notices have been criticised by many scholars as being inefficient, since they are hard to understand and data subjects do not even read them, hence they are unable to make informed decisions regarding the disclosure of their personal data.[374] One of the reasons why privacy notices have proven to be ineffective is that they revolve around the 'perfectly rational consumer with limitless attention', which has proven to be a 'false model of human capacity'.[375] Instead, human rationality is 'bounded', thus our ability to absorb information is limited.[376] Lindqvist, on the other hand, has argued that 'the form of automatic communication between smart devices makes it difficult to apply fundamental transparency and fairness principles'.[377] Thus, putting the blame on the technology itself. Carolan has also been very critical of the efficiency of privacy notices due to people's lack of capacity to understand the technological complexities of cookies. Hence, he has stated that:

> If users struggle with anything more than the most basic functions of remote control for their TVs, it is optimistic to expect them to develop an informed understanding of how different types of cookies could be implemented on different parts of different websites in a way that allows the user's data to be subject to a variety of different types of recording and analysis by a variety of different third parties. /_/ Put simply, there appears to be a limit to how much the average user can or will understand technology related issues – regardless of the level of information supplied. This obviously calls into question the veracity of a strategy that treats information about technology as the foundation of consent.[378]

Therefore, in his opinion, providing better information notices is unlikely to have any substantial effect on individual's understanding about cookies and other online activities, since

[372] ibid.
[373] Koivisto (n 369) 388.
[374] Calo (n 46) 1029.
[375] ibid 1054.
[376] ibid.
[377] Lindqvist (n 46) 2.
[378] Carolan (n 46) 469.

the online environment is so 'inherently technological' that it is an obstacle in itself.[379] Moreover, the internet changes in a fast pace, which makes it difficult not only for individuals, but also for service providers to anticipate future uses of the collected personal data.[380] In addition, he notes that the online actors have adopted a 'pro-disclosure framing' of the choice whether or not to divulge personal data.[381] Thus, 'this framing will frequently encourage agreement and disclosure by, for example, being asked for consent when their attention is focused on the benefits and rewards of the proposed course of action, rather than the more abstract privacy risks that it may involve'.[382] Furthermore, the online industry fosters a feeling of togetherness through the emphasis on peer sharing.[383] Therefore, Carolan has spoken against the use of consent in the online environment, because 'the fact that the architecture of online engagement is under the complete control of a particular party means that there are almost ever-present opportunities for users to be subtly or surreptitiously prompted in a desired direction'.[384]

Monteleone has criticised the ineptness of privacy notices as evidenced by studies conducted in Europe, which show that 'they are not effective, at least not concerning the purpose of increasing users privacy awareness (risks and rights) nor of encouraging a more responsible data disclosure'.[385] The studies show also the presence of 'privacy paradox', which means that despite users becoming increasingly aware and concerned about their online privacy, they do not read privacy policies and continue to give away personal data.[386] Monteleone suggests that the privacy paradox can be cured by implementing privacy by design technology as it inherently 'embeds fundamental privacy principles'.[387] Furthermore, she has criticised the traditional privacy notices for exposing data subjects to 'information overload'.[388] This means that an individual will be overwhelmed by excessive information, hence 'causing her to skim,

[379] ibid.
[380] ibid.
[381] ibid 470–471.
[382] ibid 470.
[383] ibid 471.
[384] ibid 472.
[385] Monteleone (n 283) 75; see also for example Lusoli Wainer and others, 'Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management' (Joint Research Centre and European Commission 2012) JRC Scientific and Policy Reports <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/pan-european-survey-practices-attitudes-and-policy-preferences-regards-personal-identity> accessed 25 February 2020.
[386] Monteleone (n 283) 75.
[387] ibid 90.
[388] ibid 104.

freeze, or pick out information arbitrarily'.[389] Thus, instead of bombarding data subjects with a lot of information companies should focus on providing good information in order to help data subjects make informed decisions.[390]

Though some critics, the more sceptic ones, are in favour of forsaking privacy notices altogether and instead have more substantive regulation,[391] there are still those who see the value of notices and who advocate the use of innovative privacy notices instead of the traditional ones.[392] For example, despite her criticism, Monteleone is against disowning privacy notices and consent altogether and believes that privacy policies can hold power if presented in an appropriate manner in the online environment and containing relevant information.[393] She has stated that 'we should try understanding the underlying reasons, the actual users' attitudes and behaviours and seek out alternative, innovative and integrated ways to enhance them'.[394] Therefore, she has contended that instead of using traditional privacy notices, which are usually in text form and have proven to be inefficient, companies should move on to using 'innovative information notices, like salient alerts and nudges'.[395] Privacy nudges are a 'software that essentially sits over your shoulder and provides real-time reminders short on-screen messages that the information you're about to send has privacy implications'.[396] She believes that using privacy nudges 'as complementary regulatory tools would seek at encouraging, at nudging a privacy-protective behaviour, while preserving the freedom of choice of the users, achieving the soft or libertarian paternalism'.[397]

Another improvement suggested by Monteleone is to use 'visceral notices', rather than traditional long text formats.[398] The aim with visceral notices is to 'have less text and more interaction' and it has proven to be 'more successful at electing privacy-protective behaviour'.[399] Calo has also recommended the use of visceral notices instead of abandoning notice method altogether. According to him these types of notices 'leverage a consumer's very

[389] Calo (n 46) 1054.
[390] Monteleone (n 283) 104.
[391] Calo (n 46) 1029–1030.
[392] see for example Calo (n 46); Monteleone (n 283).
[393] Monteleone (n 283) 76.
[394] ibid 95.
[395] ibid 75.
[396] Steve Lohr, 'Redrawing the Route to Online Privacy' *The New York Times* (27 February 2010) <https://www.nytimes.com/2010/02/28/technology/internet/28unbox.html> accessed 24 March 2020.
[397] Monteleone (n 283) 110.
[398] ibid.
[399] ibid 110, 111.

experience of a product or service to warn or inform'.[400] In his view: 'You can write a lengthy privacy policy that few will read, or you can design the website in a way that places the user on guard at the moment of collection or demonstrates to the consumer how their data is actually being used in practice.'[401]

An example of visceral notices is using an avatar that runs back and forth at the end of the webpage to alert the website visitor of third-party tracking.[402] This could be more efficient in informing the visitor of tracking than few paragraphs in privacy notices,[403] because studies have shown that 'people naturally react more strongly, in a visceral way, to anthropomorphic cues'.[404] Calo further explains that this type of notice 'attempts to create the relevant state of awareness in a sense directly', instead of using language to communicate,[405] because '[l]ike language, experience has the capability of changing … our understandings and assumptions about a given product, environment, or system'.[406] Tene and Polonetsky have also stated that visceral notice 'seeks to elicit an emotional or intuitive reaction based on a perception that a given practice is desirable or not'.[407]

Calo acknowledges also the drawbacks of visceral notices, which include the fact that they may contain 'less actionable information' than written text.[408] Hence, he suggests a combination of visceral notice for consumers and traditional written policy directed at, inter alia, experts, regulators and journalists, who may understand the technical details better.[409] According to Calo, this 'two-track system … could combat the assumption that consumers had read and agreed to longer terms, and yet preserve the advantages of transparency'.[410]

Even though the 'psychology literature offers ample evidence that the provision of information does little to enhance user understanding of how technologies of any level of complexity operate',[411] privacy notices are still a popular method for regulators to use in privacy and data

[400] Calo (n 46) 1027.
[401] ibid 1034–1035.
[402] ibid 1040.
[403] ibid.
[404] Lohr (n 396); see also Calo (n 46) 1038–1039.
[405] Calo (n 46) 1044.
[406] ibid 1034.
[407] Tene and Polenetsky (n 49) 346.
[408] Calo (n 46) 1062.
[409] ibid 1062, 1063.
[410] ibid 1063.
[411] Carolan (n 46) 468.

protection framework.[412] This is because policymakers favour the use of notices instead of adopting regulations restricting conduct, which is a more invasive option and can in turn hold back innovation.[413]

Calo has argued that, though, privacy notices have largely been deemed unsuccessful in the online context, 'the nature of digital services means that viable regulatory alternatives are few and poor'.[414] The advantage with privacy notice is that it is 'relatively cheap to implement and easy to enforce', hence it does not impose a great burden on regulator's resources.[415] Additionally, privacy notice does not prevent innovation and competition and it 'purports to respect the basic autonomy of the consumer or citizen by arming her with information and placing the ultimate decision in her hands'.[416] Hence, turning away from privacy notices completely might not constitute any better course of action. Calo argues that instead of giving up on notices legislators and industry should 'innovate around notice' and 'assess the results of such innovation'.[417]

The failure of privacy notices can also be traced to the phenomenon of 'transparency paradox'.[418] This occurs because privacy notices must be sufficiently detailed in order to make the data subject informed about the data processing purposes and methods, but this tends to result in long and complicated privacy statements, which are instead ignored by data subjects.[419] On the other hand, short and summarised privacy notices lack enough details to provide data subjects with enough facts so he or she can make an informed decision whether or not to consent.[420] This paradox could potentially be reduced by using privacy notices where the text is presented in a layered form, as has been emphasised by the WP29.[421] Nevertheless, it can still be difficult to fulfil requirements of both detailed and easy to understand information.

[412] Calo (n 46) 1027.
[413] ibid 1030, 1048, 1071.
[414] ibid 1031.
[415] ibid 1048.
[416] ibid 1048, 1049.
[417] ibid 1072.
[418] Betkier (n 353) 34–35.
[419] ibid.
[420] ibid.
[421] see Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 35.

People's interest in cookie policies and practices can be paralleled with people's interest in their data protection by looking at whether there has been a significant increase in complaints to data protection authorities and whether people have started to read privacy notices over the past year. The European Commission published on 25 January 2019 an infographic on GDPR compliance and enforcement.[422] The infographic shows that since the GDPR came into force 95 180 queries and complaints have been lodged to data protection authorities by individuals or organisations taking action on behalf of data subjects. The lodged complaints concerned mainly telemarketing, promotional emails and video surveillance.

Nearing the first year-anniversary of the GDPR the European Commission published on 22 May 2019 another infographic on GDPR compliance and enforcement.[423] The infographic shows that the lodged complaints to data protection authorities had increased to a total of 144 376. It can be seen that people's interest and activity had increased a lot even within five months, which can be taken as a positive sign that people are more engaged in monitoring and alerting any misuse of their personal data. Hence, it is possible that people will also be more mindful and engaged in the future with respect to cookie practices. The drawback with this infographic is, however, that it does not show how many complaints were lodged under the Data Protection Directive. Thus, though this number of lodged complaints under the GDPR seems big, there is no comparison as to what the number was in the pre-GDPR era and hence, whether it has increased or decreased.

The Special Eurobarometer shows that there has been an increase in people's reading of privacy notices.[424] The study shows that 60% of the respondents, who use the internet, read website's privacy statements, though mainly partially. Only 13% read the privacy statements completely. Interestingly, however, the study also revealed that compared to the 2015 study, people are now less likely to read privacy statements, whether partially or fully.[425] The main reason for not reading privacy statements fully or at all is that people find them too long (66%) and

[422] 'GDPR in Numbers' (European Commission, 25 January 2019) <https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf> accessed 22 April 2020.
[423] 'GDPR in Numbers' (European Commission, 22 May 2019) <https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf> accessed 4 April 2020.
[424] see European Commission, 'Special Eurobarometer 487a: The General Data Protection Regulation, Full Report' (n 284) 47.
[425] ibid.

complex or unclear (31%). Some people (15%), on the other hand, believe that the law will come to their rescue anyhow.[426]

Additionally, the study shows that 56% of social network users have attempted to change their privacy settings, but this proportion has also slightly decreased compared to 2015.[427] The reasons for not changing privacy settings are mainly that the users either trust that the social network will have adequate privacy settings in place or that they do not know how to change the default settings.[428] It is interesting that despite all the promotion of the GDPR,[429] people's activity in terms of reading privacy policies or changing their privacy settings have decreased slightly from the period when data protection was not yet a hot topic. It could, however, be inferred that this is because people trust the new legislation will protect them better and so they do not have to exercise supervision as actively anymore.

4.3 SUMMARY OF THE ISSUES WITH COOKIE CONSENTS AND NOTICES

It is quite inevitable that users will have to sacrifice, at least to a certain extent, their personal data when entering the internet, since many website services are fuelled by personal data and the internet has basically become a necessity in the modern developed world. From the discussion above, however, it can be seen that there are numerous issues with consent and notice, especially in the online environment. These issues are summarised below.

i) *Information Asymmetry:* Users are rarely aware of how companies use their data.
ii) *Transaction Costs:* Users do not read privacy and cookie notices as they tend to be lengthy, difficult to understand and unclear. Hence, familiarising themselves with the information would be too time consuming.
iii) *User's Bounded Rationality and Skewed Decision Making*: People's rationality is limited, and their decision making is influenced by biases, rules of thumbs, heuristics and other factors. Hence, users are not equipped to make rational choices.

[426] ibid 51.
[427] ibid 56.
[428] ibid 63.
[429] 'GDPR in Numbers' (n 422) according to this 67% of Europeans have heard of the GDPR.

iv) *The Problem of Scale*: Internet users are exposed to too many consent requests, which makes privacy management on various websites difficult for them to handle due to lack of time and resources.

v) *The Aggregation Effect*: User's data given in isolation can later be combined and the aggregate of these combined data can reveal new or sensitive information.

vi) *Technological Complexity of the Internet and Cookies:* The internet and cookie technology are so complex that people lack understanding despite being informed through privacy and cookie notices.

vii) *Privacy Paradox*: Despite being aware of privacy risks people still continue to disclose their personal data online.

viii) *Transparency Paradox*: It is difficult to make privacy and cookie information both clear and reader friendly and at the same time comprehensive in order to enable the user to make an informed decision on whether or not to consent.

ix) *Network Effect*: People are reluctant to leave big online social communities regardless of privacy risks, since all their friends and peers are there. Furthermore, similar alternative services might not exist in the online environment, especially when it comes to the popular ones, like Facebook, Instagram and LinkedIn.

Due to all of these listed issues with consent and notice, it has therefore been argued that 'consent is a burdensome mechanism to use in the online environment and may be seen as losing the conditions of validity'.[430] This supports the first hypothesis of this thesis that consent and notice practices under the current data protection framework do not provide effective control and protection to individuals when processing personal data obtained via internet cookies. Consequently, the traditional model of consent and notice system might not always be the appropriate tool for processing data obtained through cookies. Nevertheless, at the moment it is difficult to see that consent would be removed as the legal basis for cookies as it is so enshrined in the legal culture of data protection.

This thesis is not, however, of the opinion that consent should be disregarded altogether with respect to cookies, but the consent and notice mechanism should be improved in order to be more efficient. For example, different types of cookies could better benefit from having different legal basis, instead of pushing for one legal basis for all types of cookies. This thesis

[430] Betkier (n 353) 36.

does see the value in consent in certain circumstances, such as with respect to analytics, tracking and behavioural advertising cookies provided that the user or visitor is properly informed. Cookies, which are necessary for the functioning of the website, might benefit from another legal basis, for example, the legitimate interest, or even legal obligation, especially with respect to cookies used for combatting abuse and fraud. Instead of providing a long list of different cookie purposes for which user's consent is needed, regardless if this is provided in a granular form, it would be better to narrow down those cookies that should actually be subjected to consent. This could already help improving data subject's understanding of what he or she is consenting to and thus facilitate valid informed consent.

The issue with third parties placing cookies on user's terminal equipment is that they are silent partners hiding in the shadows. Thus, though the user could reasonably expect that the website he or she is visiting might track his or her movements whilst being on that website, it is not reasonable to expect that the user would know or be aware of all the silent partners that might also be tracking him or her, especially across multiple domains.

This thesis argues that the cookie notice should explain better what behavioural advertising means in practice as users might not understand that personalised advertisement is the result of tracking their behaviour and preferences on the internet. Furthermore, with respect to third party advertising cookies, it should be explained to the users that they are tracked across multiple websites by the same advertising network agency, in order to see what they are interested in, which in turn enables the provision of personalised advertisement. This would alert the users that they are being monitored by the same entity even on different websites.

If websites adopt Calo's example of visceral avatar notice, then the third party advertising agency could use the same avatar on all those websites it has an agreement with. This would provide a more visual notice to the user and inform him or her as to which advertising network is monitoring him or her on that specific website. If the advertising network agency has high privacy protective features and becomes known for it, then the avatar could serve as, or become similar to a trademark for its data protection features. Thus, though traditional privacy notices have been deemed inefficient, there is also room for improvement for more innovative notices, rather than discarding notice method completely.

5 Cookie Consents and Notices in Practice

Different technological means can be used to obtain consent for cookies and the WP29 has recognised that website operators are free to choose the practical implementation best suited for them and their target audience.[431] The important thing is that 'consent can be deemed as valid under EU legislation'.[432] This chapter will provide practical examples of how different websites from the legal and public sector present their cookie consent requests, in order to analyse whether or not they fulfil the consent requirements under the EU data protection regime. Of course, the consent mechanisms will diverge depending on what type of cookies are used and for what purposes. The thesis will not provide an in-depth analysis of the full cookie notices. Instead, the analysis will focus more on the short text supplementing the cookie consent request, as this tends to be the first information that users see with respect to cookies.

5.1 NATIONAL DATA PROTECTION AUTHORITIES

5.1.1 The UK

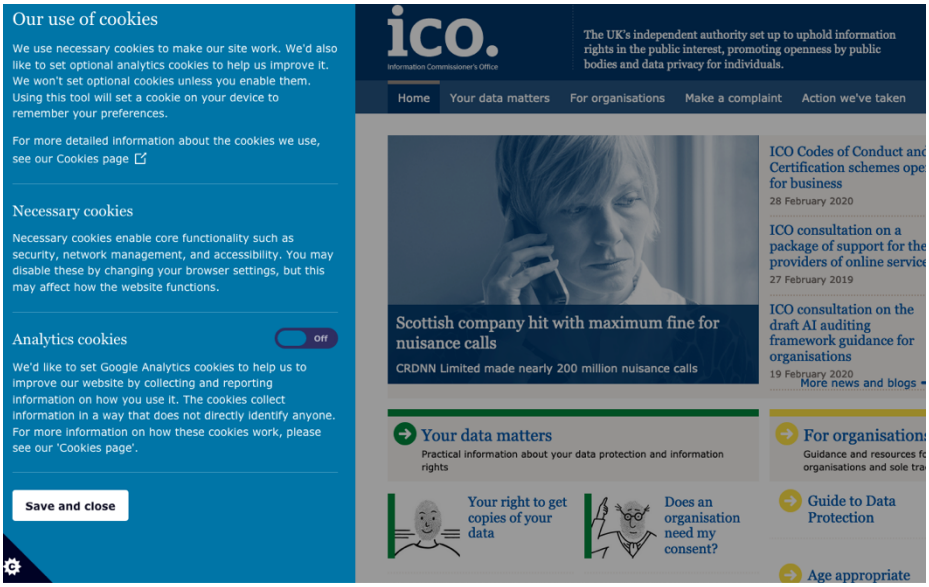

Figure 1. The Information Commissioner's Office (ICO) - Cookie Consent Request

As seen from Figure 1, the cookie consent request for the Information Commissioner's Office (hereafter the 'ICO'), which is the UK's independent data protection authority,[433] pops-up from the left of the website. Users can also view it again by clicking on the 'C' icon, thus making it

[431] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 2.
[432] ibid.
[433] see 'Information Commissioner's Office' (12 February 2020) <https://ico.org.uk/> accessed 17 February 2020.

easy for users to change their minds with respect to consenting to analytics cookies. Furthermore, the slider is by default on 'Off' mode, hence corresponding to Recital 32 of the GDPR and the CJEU's judgment in *Planet49*, where pre-ticked boxes were rejected as constituting valid consent. In order for analytics cookies to be placed on the user's device the user must actively set it on 'On' mode. The ICO explains also briefly the differences between necessary and analytics cookies and the accept button is clearly set beside the explanation of the analytics cookies. This will make it easier for the user to understand that his or her consent will only affect the analytics cookies and not necessary cookies. The full cookie notice can be found from behind the 'Cookies page' hyperlink under 'Our use of cookies' and in the footer of the website.[434] Thus, the ICO has provided visible information and easy access to it.

One criticism is, however, that though the ICO states that necessary cookies can be disabled through browser settings, it does not provide any further advice on where or how to do this. This information can, however, be found from the full cookie notice. This thesis argues that it would be clearer if the information about the necessary cookies would also refer to the hyperlink or have a brief explanation on how or where to change the browser settings. On the other hand, since this concerns necessary cookies and Article 5(3) of the ePrivacy Directive has exempted these types of cookies from consent, it is argued that this is not a big offence.

Another criticism is that the user must make a choice to either leave the slider on its default position or change it and then click on 'Save and close', before the user can continue using the website. This could be considered as a mild version of cookie walls, as the user is forced to make a choice. On the other hand, the user has a real choice on whether or not to accept the cookie analytics. Additionally, this seems to provide only little disturbance on user experience as the user can just click on 'Save and close' immediately, in which case no analytics cookies are installed as this is the default position. This conforms with the WP29's opinion that cookie consent request 'should not be *unnecessarily* disruptive to the use of the service for which the consent is provided'.[435] All in all, the ICO seems to have a valid cookie consent mechanism in place with prior and clear accessible information at least with respect to analytics cookies.

[434] see ICO's cookie notice from 'Cookies' (8 January 2020) <https://ico.org.uk/global/cookies/> accessed 3 March 2020.
[435] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 16 original emphasis.

5.1.2 Belgium

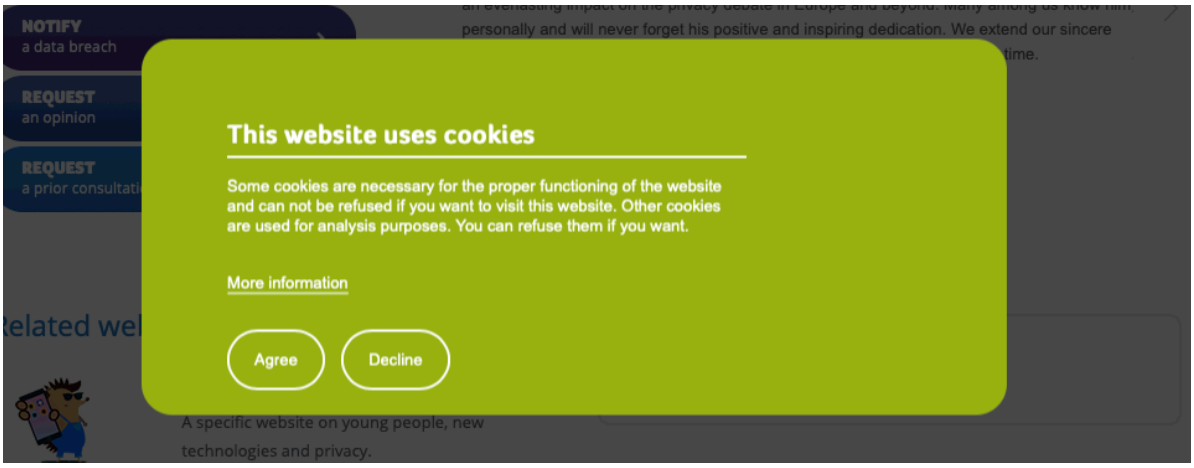

Figure 2. Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA) - Cookie Consent Request

As seen from Figure 2, the Belgian data protection authority (hereafter the 'APD-GBA') has a cookie pop-up screen in the middle of the website, with a brief explanation about the necessary and analytics cookies.[436] The APD-GBA seems to also use a mild level of cookie walls, since a user cannot continue to the website until he or she actively clicks on either 'Agree' or 'Decline' button. It should be noted, however, that neither button is highlighted, hence providing a fairer choice, than other websites who use highlighted 'accept' buttons, because arguably data subject's eyes tend to register to the highlighted button first and hence he or she might be subconsciously influenced to click on that button.

The modal dialogue box includes a hyperlink for more information about cookies, however, there is no cookie policy in the footer of the website, only a privacy statement. The cookie policy can be found from within the privacy statement, but it does take some navigation to find it. Hence, the information is no longer easily accessible after the choice whether or not to consent to cookies has been made. Furthermore, it is difficult to find the choice mechanism again in case the user changes his or her mind. The APD-GBA does not provide an option for the user to disable the necessary cookies unlike the ICO. But, since necessary cookies are exempted from consent, this does not violate the ePrivacy Directive. Thus, the Belgian data protection authority seems to provide a valid consent mechanism, except for the accessible information, which should be prominent even after the choice has been made.[437]

[436] see 'Data Protection Authority' <https://www.dataprotectionauthority.be/> accessed 17 February 2020.
[437] see Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 43) para 11.

5.1.3 Sweden

Figure 3. Datainspektionen - Cookie Consent Request

Figure 3 shows the bottom of the website for the Swedish data protection authority.[438] The cookie text states that the data protection authority uses cookies and the visitor chooses whether he or she accepts them. The text continues with a link to further information highlighted in red. Though, the information informs the visitor that it is up to him or her to accept the cookies it does not provide any 'accept' or 'decline' button immediately after, or in close proximity to the text, nor does it provide information on where to change the cookie settings. Furthermore, the cookie information is displayed with quite small text in black on the bottom of the website, hence it is not very eye catching and instead blends quite easily in there. There is another hyperlink for cookie information in red ('Användning av kakor') under the header for information about the data protection authority. Though, this is in red so are the other hyperlinks, thus blending in as well.

There does not seem to be any prior consent mechanism in the first place, therefore it is in conflict with Article 5(3) of the ePrivacy Directive. The full cookie policy does, however, contain information on how to change browser settings to reject cookies. Thus, it could be argued that this website uses an opt-out model, which is no longer acceptable under the revised Article 5(3) of the ePrivacy Directive. Hence, the Swedish data protection authority has failed to comply with the EU cookie rules.

[438] see Datainspektionen, 'Datainspektionen' <https://www.datainspektionen.se/> accessed 3 March 2020.

5.1.4 Spain

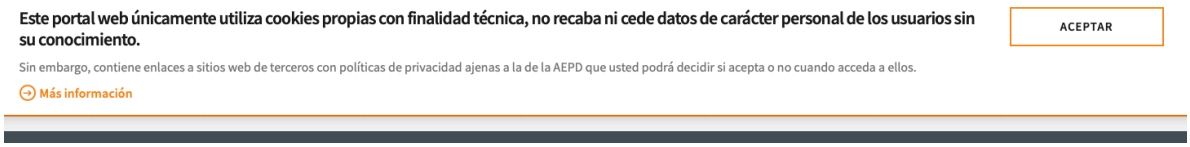

Figure 4. Agencia Española de Protección de Datos (AEPD) - Cookie Consent Request

Figure 4 shows the header of the website of the Spanish data protection authority (hereafter the 'AEPD').[439] It uses a pop-up banner with a brief statement that the website uses its own cookies for technical purposes only and contains links to third party websites, who will ask separate consents when accessing them. The AEPD has only an 'accept' button and no 'decline' button, hence users do not really have any other choice but to accept the technical cookies. This would not constitute valid consent, since at least the element of 'freely given' is absent.

Technical cookies can, however, be considered necessary to enable the proper functioning of the website and therefore be exempted from the consent requirement under the ePrivacy Directive. On the other hand, since the data subject's consent will not really have any impact, it is questionable whether consent should be asked in the first place if no real choice is given. In this case consent does not seem to be the appropriate legal basis. Alternatively, it should be made clear that these types of cookies do not even require user's consent under EU law.

5.1.5 France

The French data protection authority's website (hereafter the 'CNIL')[440] seems to have a detailed consent request mechanism for third party cookies as seen from Figure 5. The website does not seem to use any pop-up banner, instead the user must click on 'Cookies Management' up on the right corner or in the footer. This provides an easy access for changing the cookie settings. It also provides a brief explanation about the third party cookies used by the website and the user can choose to accept or decline all third party cookies at once or service by service. This allows the user to decide which purposes it accepts and which it refuses, hence enabling specific and free consent based on prior information. Neither the 'Allow' or 'Deny' button is

[439] see 'Agencia Española de Protección de Datos | AEPD' <https://www.aepd.es/es> accessed 17 February 2020.
[440] see 'Homepage | CNIL' <https://www.cnil.fr/en/home> accessed 17 February 2020.

highlighted, though they have different colours (blue and red respectively). Therefore, it can be argued that the user is free from influence.

The default position seems to be that third party cookies are denied, unless the user consents, since the text states that '[i]f you give your consent', thus adopting a prior op-in consent method. There is a link to further information at the end of the modal dialogue box. The method seems to be conforming with all of the requirements for a valid consent. Apparently the CNIL does not use any first party cookies as it only mentions third party sites.

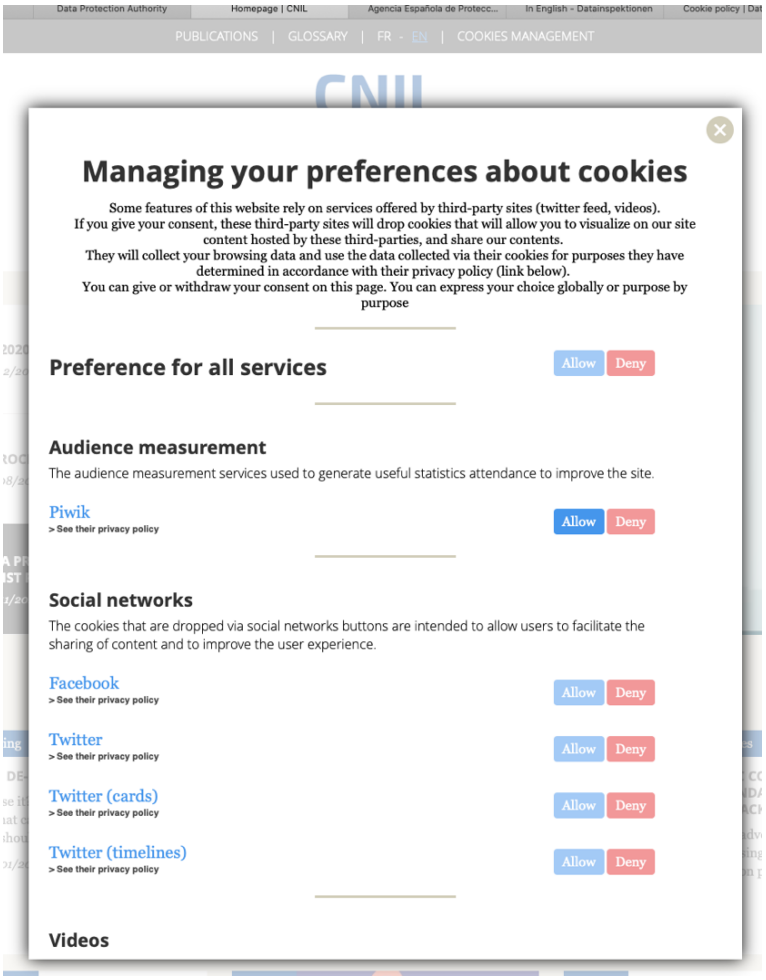

Figure 5. Commission Nationale de l'Informatique et des Libertés (CNIL) - Cookie Consent Request

5.1.6 Conclusion

The above examples have demonstrated that there is some inconsistency in cookie practices among the national data protection authorities. This can of course depend to a certain extent on the differences in national implementations of the ePrivacy Directive. Nevertheless, these examples show that there seems to be some ambiguity with respect to the consent exemptions,

especially regarding cookies that are considered necessary for the website's functioning. For example, the Spanish website provided an (ineffective) accept button for them, while others did not, and though the UK did not ask for consent, as necessary cookies are exempted from consent under the ePrivacy Directive, it did provide an opportunity to disable them, while others did not.

This thesis argues that only the UK and France and maybe Belgium could be considered fully compliant with the cookie rules under the EU with respect to the type of cookies used. Due to the inconsistency, however, it can be argued that the GDPR and the ePrivacy Directive have not succeeded in providing clear cookie rules and bringing harmonization, thus supporting the second hypothesis of this thesis. Hence, better clarification is needed, since even data protection authority websites struggle with cookie compliance. Furthermore, if the Member States are not in consensus of what constitutes the correct cookie practices under the EU data protection laws, then this will be very onerous on the companies, who must tailor their cookie practices in accordance with all the national laws where they operate their websites. This practice is neither business friendly nor effective.

5.2 LAW FIRMS

5.2.1 Roschier

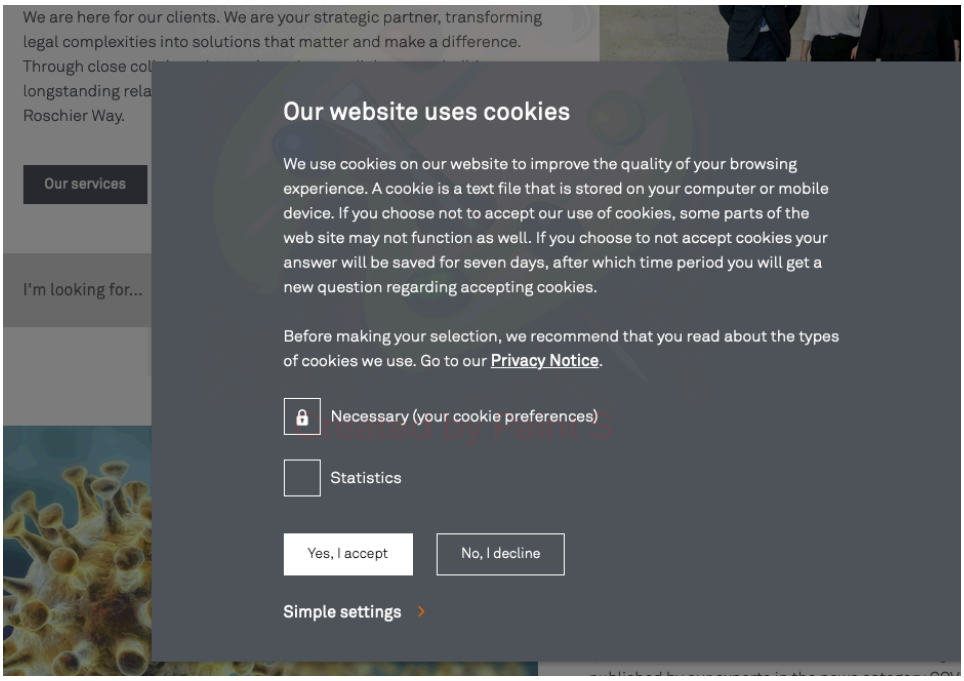

Figure 6. Roschier - Cookie Consent Request

The law firm Roschier seems to also use a mild version of a cookie wall.[441] The cookie text pops-up in the middle of the website and user must click on 'accept' or 'decline' button before he or she can continue to the website. The 'accept' button is highlighted, which can provide an unfair image, as the website seems to be trying to direct the user to accept the cookies. Necessary cookies are locked, which is acceptable, since they are allowed without user's consent under the ePrivacy Directive Article 5(3). The request for consent seems to, however, cover even these cookies, because the text states that 'If you choose not to accept our use of cookies, some parts of the web site may not function as well.' It is doubtful that refusal of statistics cookies would affect the functioning of the website. This is further clarified in the full cookie notice, which states that refusal of strictly necessary cookies will prevent the proper functioning of the website. The user does not, however, have real choice with respect to the necessary cookies, since the choice is locked. Instead of referring to necessary cookies in the consent request, the text should make it clear that these cookies are allowed under EU law.

The user has a choice with respect to the statistics cookies and the purpose is separated from the necessary cookies. The box is not pre-ticked and thus it requires user's active input. Hence, Roschier seems to meet the conditions of valid consent under the GDPR with respect to the statistics cookies. Another criticism, however, is that the cookie notice is embedded in the Privacy Notice. The cookie notice is, however, easy to find from the privacy notice as it is layered, and the cookie notice has its own heading. Nevertheless, the website could consider providing the cookie policy its own hyperlink in the footer, in order to make it more accessible. In conclusion, the consent request for the statistics cookies seems to comply with the requirements of valid consent. The text regarding the necessary cookies should, however, be clarified.

[441] see 'Roschier - Leading Law Firm in the Nordic Region' (*Roschier*) <https://www.roschier.com/> accessed 17 February 2020.

5.2.2 Hannes Snellman

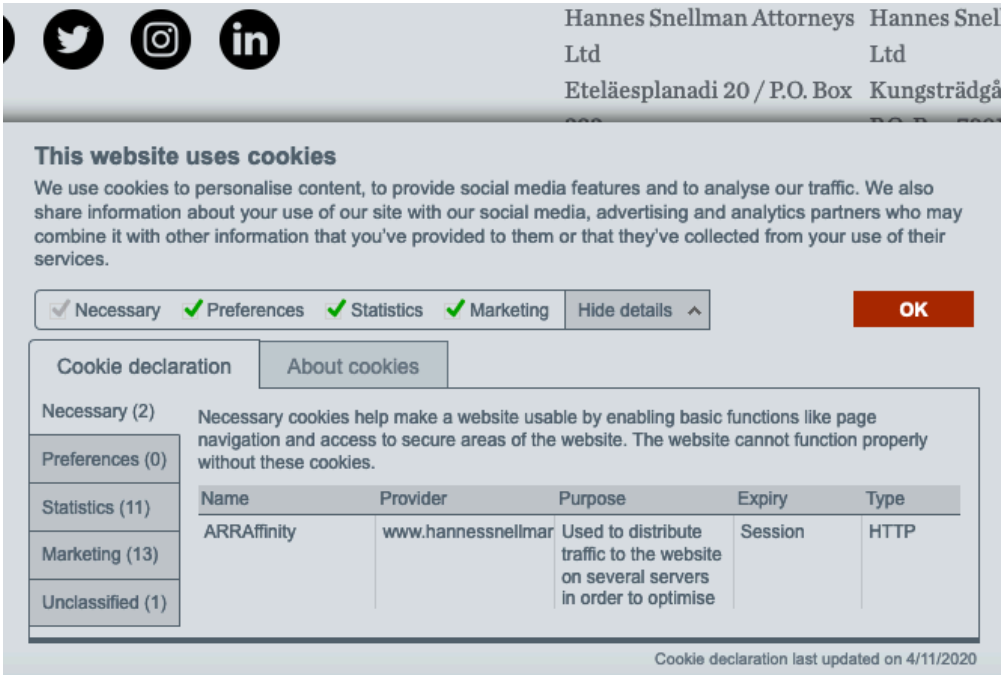

Figure 7. Hannes Snellman - Cookie Consent Request

The website of the law firm Hannes Snellman[442] uses layered information and granular choice in its cookie consent request that pops-up from the bottom of the website. The user can read more about the different cookies by surfing the left column, thus the requirement of being informed is complied with. The full cookie policy is found from behind the link in the footer of the website and the user can change the consent settings from there as well, hence making it easy for the user in case he or she has a change of heart.

The cookie consent mechanism conforms also with the requirement of specific consent as the different purposes are separated and the user can choose which he or she accepts. It should be noted, however, that all of the different purposes are automatically ticked, hence the user must deselect them in order to not consent. This is disapproved under Recital 32 of the GDPR and would not be considered a valid consent after the decision by the CJEU in the *Planet49* case, as discussed above. The necessary cookies are locked on this website and though acceptable, because they are exempted from the consent requirement under the ePrivacy Directive, this thesis thinks that the text could clarify this.

[442] see 'Hannes Snellman - Home' <https://www.hannessnellman.com/> accessed 17 February 2020.

5.2.3 Bird & Bird

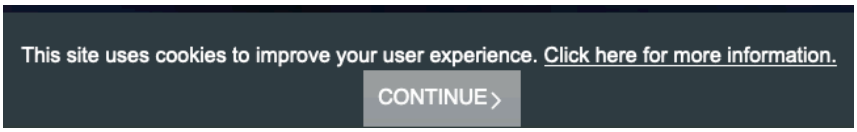

Figure 8. Bird & Bird - Cookie Consent Request

In contrast to the two law firms above, the multinational law firm Bird & Bird provides a very brief pop-up text in the footer of its website.[443] The site does not, however, ask for any consent. It merely provides a 'Continue' button and a link to further information. Clicking on the link to further information will not constitute consent as has been clarified by the WP29.[444] Furthermore, merely continuing on the website does not constitute consent either.[445] It is inferred that the website uses an opt-out method, because no consent is requested and the full privacy and cookie policy states that 'On your first visit to this website you will have seen a pop-up to inform you about the purposes for which cookies are being used and the means to opt-out.'[446] Thus, this website is in conflict with Article 5(3) of the ePrivacy Directive, which requires prior opt-in consent. This website has also embedded cookie policy into its privacy notice. The text would be clearer and easier to navigate if it offered layered information or a separate cookie notice.

5.2.4 Borenius

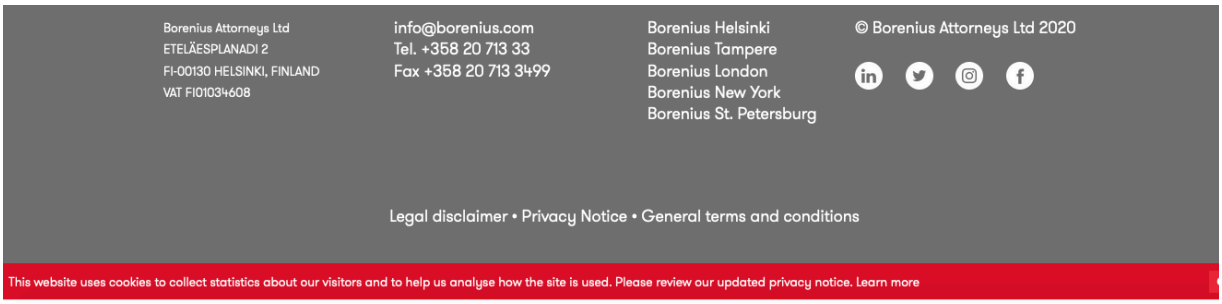

Figure 9. Borenius - Cookie Consent Request

[443] see 'Bird & Bird - International Law Firm' (*Bird & Bird*) <http://www.twobirds.com/> accessed 17 February 2020.
[444] Article 29 Data Protection Working Party, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 42) 5.
[445] see Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 15–16; Opinion of AG Szpunar in *Planet49* (n 71) para 66.
[446] see 'Cookies Policy' (*Bird & Bird*) <http://www.twobirds.com/en/more-information/cookies-policy> accessed 27 April 2020.

The law firm Borenius uses a similar method as Bird & Bird,[447] as it has also a brief pop-up text in the footer, which explains that cookies are used to 'collect statistic about our visitors and help us analyse how the site is used'. No consent is asked, only an 'OK' button is provided. This can be acceptable if the data is anonymized, as such data falls outside the scope of the GDPR. In fact, Recital 26 of the GDPR has stated explicitly that anonymous information used for statistical purposes falls outside its scope. Thus, in this case the law firm does not need to ask for consent. Nevertheless, the text at hand could be made clearer by including a statement that the website collects only anonymous data. This is explained in the full privacy notice, which incorporates information on cookies as well. A separate cookie notice would be recommended, or the use of layered information in the privacy notice, since at the moment it takes some navigation to find the cookie information.

5.2.5 Deloitte

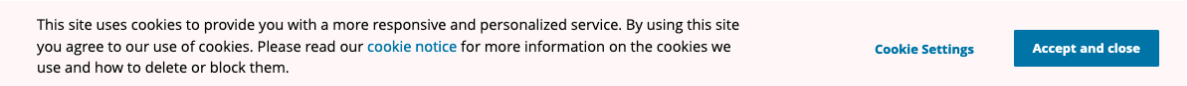

Figure 10. Deloitte - Cookie Consent Request

The law firm Deloitte[448] has a pop-up banner in the header which states, among others, that 'By using this site you agree to our use of cookies.' This is accompanied by a highlighted 'Accept and close' button, but no reject option as seen from Figure 10. Such practice has been disapproved by the WP29,[449] as mentioned above and this does not really give the user any real choice with respect to the use of cookies and therefore does not provide a valid consent. Furthermore, as mentioned above, the CJEU in *Planet49* confirmed that consent must be separate from another act.[450] Hence, the act of continuing surfing the website cannot at the same time indicate consent to the use of cookies.[451] It is, however, possible that this text covers only the necessary cookies, since the pop-up banner does provide a link to 'Cookie Settings'.

The cookie settings, as seen from Figure 11 and 12, provide a more detailed consent option, layered information and the possibility to consent to separate purposes one by one or all at

[447] see 'Borenius' (*Borenius*) <https://www.borenius.com/> accessed 17 February 2020.
[448] see 'Deloitte | Audit, Consulting, Financial, Risk Management, Tax Services' (*Deloitte*) <https://www2.deloitte.com/global/en.html> accessed 17 February 2020.
[449] see Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 144) 15–16.
[450] *Planet49* (n 174) para 58-59; see also Opinion of AG Szpunar in *Planet49* (n 71) para 66.
[451] *Planet49* (n 174) para 58-59; see also Opinion of AG Szpunar in *Planet49* (n 71) para 66.

once. The strictly necessary cookies are 'Always Active', as seen from Figure 11. Hence, the text in the pop-up banner might refer to these cookies only, because the other cookies are by default on 'inactive' mode (see Figure 12 for an example). Therefore, Deloitte applies an opt-in consent system for other than necessary cookies (which might not need consent in the first place). The cookie settings provide an immediate and clear advice on where the user can go and change his or her preferences. The cookie notice is also in the footer of the website and the full text provides a link to the cookie settings. Hence, the information and the cookie settings are at all times easily available. The cookie consent mechanism seems to comply with the consent requirements, though even Deloitte could clarify that the necessary cookies are permissible without user's consent under EU law and therefore they can be installed.

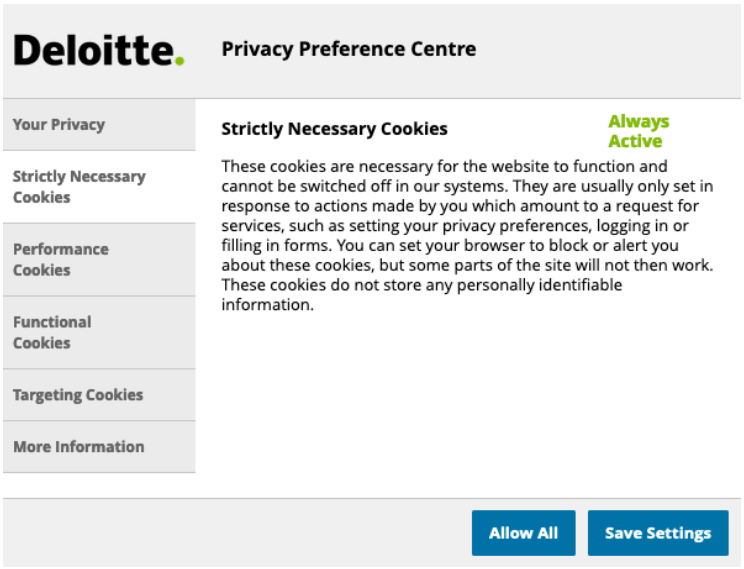

Figure 11. Deloitte - Cookie settings - Necessary cookies

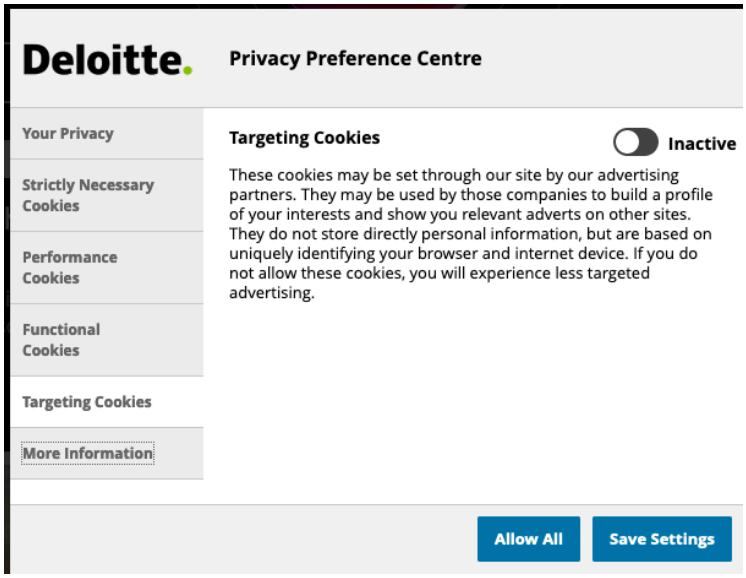

Figure 12. Deloitte - Cookie settings - Targeting cookies

5.2.6 Conclusion

The above examples show that there is also some inconsistency of cookie practices among law firms and at least one of them had incorporated an opt-out method, which is no longer acceptable under Article 5(3) of the ePrivacy Directive. Furthermore, only three law firms provided the recommended layered information on their website. It is argued that possibly three of the above examined law firms (Roschier, Borenius and Deloitte) could pass the consent test.

This thesis is of the opinion that the cookie rules are not sufficiently clear and harmonised, since even law firms apply them inconsistently and struggle with compliance, thus supporting the second hypothesis of this thesis. The fact that law firms in Finland apply different cookie practices may very well result in the giving of different advices to companies and organisations on cookie policies and practices within the country. Hence, it is important that cookie rules are clarified so that law firms can also give better legal advice to their customers.

6 The Future of Cookie Legislation

EU citizens, consumers and civil society organisations have expressed their dissatisfaction with the ePrivacy Directive in a public consultation conducted by the European Commission in 2016.[452] Their dissatisfaction concerned, among others, the inconsistent interpretation and enforcement of the ePrivacy Directive due to differences in national implementations.[453] This supports the second hypothesis of this thesis that the ePrivacy Directive has failed to harmonise the rules on cookie consent. Additionally, the respondents were also critical of cookie rules, which in their opinion did not provide sufficient protection as 'consumers are not offered real choice to accept cookies'.[454] This in essence supports the first hypothesis of this thesis that cookie consent rules under the current data protection framework do not provide effective control and protection to individuals when processing personal data obtained via internet cookies. Hence, consent might not always be the appropriate legal basis for processing data obtained via cookies, especially if the ensuing control is illusory.

The proposed ePrivacy Regulation is hopefully going to bring better clarity and harmonisation with respect to the processing of data in the electronic communications sectors, including the use of cookies. The first draft of the ePrivacy Regulation was adopted on 10 January 2017,[455] with the intention to replace the ePrivacy Directive and thus become a *lex specialis* legislation to the GDPR. The proposal has, however, undergone many revisions during the different EU Council Presidencies and has not yet been passed, as the Member States struggle to reach an agreement.[456] Thus, it has been speculated that its enactment might be pushed to even 2023.[457]

6.1 COOKIE WALLS

The Finnish Presidency's amended draft version of the ePrivacy Regulation was adopted on 15 November 2019, but this has also been rejected.[458] One of the disagreements in this draft proposal between the Member States concerned cookie walls and 'the need not to undermine

[452] see 'Synopsis Report of the Public Consultation on the Evaluation and Review of the EPrivacy Directive' (European Commission 2016) <https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive> accessed 18 September 2019.
[453] ibid 2.
[454] ibid.
[455] ePrivacy Regulation draft January 2017 (n 13).
[456] see for example 'EPrivacy Regulation' (n 14) and; 'EU EPrivacy Regulation' (n 14).
[457] 'EPrivacy Regulation' (n 14).
[458] Jennifer Baker, 'How the EPrivacy Regulation Talks Failed ... Again' (26 November 2019) <https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/> accessed 29 November 2019.

existing business models'.[459] The draft text was criticised for not providing sufficient data protection to individuals and instead supporting online ad networks and facilitating the monopoly exercised by big tech companies.[460] Cookie walls, also called 'tracking walls', require website visitors to accept cookies used by the website (this may also include third party cookies) or otherwise they will be denied access to the website's service.[461] Thus, cookie walls provide a take-it-or-leave-it type of choice, which has been criticised by the WP29 and legal academics as seen above.[462] The WP29 has recommended that cookie walls be banned under the ePrivacy Regulation as these kind of practices are 'rarely legitimate',[463] and they would not satisfy the condition of 'freely given' consent under the GDPR.[464]

Carolan criticised the older forms of consent under the Data Protection Directive and the ePrivacy Directive and contended that 'The fact, for example, that the exercise of the right to withhold consent could sometimes result in a denial of access to the service in question left the user with a take-it-or-leave it choice of questionable voluntariness or value.'[465] Other critics have also claimed that it is 'debatable whether people have meaningful control over personal information if they have to consent to tracking to be able to use services or websites'.[466] Thus, they recommended that cookie walls be banned at least partially or even completely.[467]

Furthermore, the Eurobarometer survey conducted in July 2016 showed that the majority of the respondents (64%) did not think it was acceptable that companies monitor their online behaviour in exchange for free website content.[468] This thesis is of the opinion that the EU legislators should seriously consider to prohibit cookie walls altogether as a general rule and if necessary to make strict exceptions to this rule, as it seems unfair to force user's hand to click

[459] ibid.
[460] ibid.
[461] Frederik J Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the EPrivacy Regulation' (2017) 3 European Data Protection Law Review (EDPL) 353, 355 <https://heinonline.org/HOL/P?h=hein.journals/edpl3&i=382> accessed 31 March 2020.
[462] see for example Zuiderveen Borgesius and others (n 461); Carolan (n 46).
[463] Article 29 Data Protection Working Party, 'Opinion 01/2017on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)' (adopted on 4 April 2017) WP 247 15 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140> accessed 20 February 2020.
[464] Article 29 Data Protection Working Party, 'Opinion 03/2016 on the Evaluation and Review of the EPrivacy Directive (2002/58/EC)' (adopted on 19 July 2016) WP 240 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf> accessed 20 February 2020.
[465] Carolan (n 46) 465.
[466] Zuiderveen Borgesius and others (n 461) 353.
[467] ibid 368.
[468] European Commission, 'Flash Eurobarometer 443: E-Privacy, Full Report' (2016) Question 5.1 <https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy> accessed 31 March 2020.

on the cookie 'accept' button. Furthermore, since consent to cookie walls could not be considered valid under the GDPR as it is not given freely, they also fail to provide effective control and protection to internet users. This in turn is against the whole spirit of the EU's data protection regime, since its purpose is to protect user's personal data and bestow upon users increased control over their personal data.[469]

6.2 LEGITIMATE INTEREST

The Croatian Presidency is the new successor to take on the challenges of the ePrivacy Regulation in 2020.[470] It has released a revised draft of the ePrivacy Regulation on 21 February 2020 with substantial amendments to Articles 6 and 8 concerning the processing of metadata and use of cookies respectively.[471] It has not, however, addressed the issue of cookie walls in this revised draft, hence this issue remains. One of the pivotal suggestions[472] made by the Croatian Presidency is to enable controllers to rely on the legitimate interest legal basis when 1) processing electronic communications' metadata and 2) installing cookies on website user's devices, provided that additional conditions and safeguards are put in place.[473] These additional safeguards include: a) completing an impact assessment and where appropriate consult the national data protection authority, b) prohibition to disclose information to third parties (except its processors), unless the data has been anonymized, c) implement appropriate security measures, and d) inform the user of these processing activities and of the right to object to such processing.[474] Furthermore, the controller would have to complete a balancing of interest test if it intends to use this legal basis.[475] This is in accordance with Article 6(1)(f) of the GDPR.

Recital 21b of the draft ePrivacy Regulation supports the new Article 8(1)(g), which introduces the legitimate interest ground for cookies. The recital recognises that 'maintaining or restoring the security of information society services or of the end-user's terminal equipment, or

[469] see for example GDPR Recitals 6, 10 and 108; ePrivacy Directive Recitals 2, 5, 24 and 25.
[470] Baker (n 458).
[471] see Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2020) 5979/20 1; 'EU Council Presidency Releases Proposed Amendments to Draft EPrivacy Regulation' (n 15).
[472] 'EU Council Presidency Releases Proposed Amendments to Draft EPrivacy Regulation' (n 15).
[473] ePrivacy Regulation draft 2020 (n 469) Articles 6b(1)(e) and 8(1)(g); see also Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2020) 6543/20 (Consolidated version).
[474] ePrivacy Regulation draft 2020 (n 469) Recital 21c and Articles 8(1a) and 8(1a)(a)-(c).
[475] ibid Recital 21b and Article 8(1)(g).

preventing fraud or detecting technical faults might constitute a legitimate interest of the service provider'. Similarly, the recital recognises that online newspapers or other services that protect the freedom of expression and that are wholly or mainly funded by advertisements instead of monetary payment could also rely on the legitimate interest legal basis. The revised draft provides also instances when websites cannot rely on the legitimate interest legal basis. These include, inter alia, if cookie information is used for profiling purposes or for processing sensitive personal data.[476] These prohibitions are in line with the GDPR, as legitimate interest is not a possible legal basis in these circumstances.[477]

The EU Council Presidency's proposal seems to, however, go against the EDBP's advice delivered already in 2018, where it expressed its view against the use of legitimate interest ground with respect to the processing of electronic communications data and use of cookies.[478] In its view, this was one of the 'open-ended grounds', which should be excluded under the ePrivacy Regulation.[479] The draft has also received criticism from some data protection advocates who see the use of the legitimate interest ground as diminishing the level of data protection in the legislation.[480] Pirate Party MEP Patrick Breyer has stated that: 'Corporations have no "legitimate interest" in intercepting and exploiting information on our private communications and tracking our Internet use. This is none of their business.'[481] This thesis agrees with Breyer's statement to the extent that companies should not exploit this ground to process personal data extensively, for tracking purposes or beyond what is necessary for their legitimate business interests. Hence, it thinks that the legislators should clarify the circumstances when legitimate interest can be used and when consent should be used instead.

Borgesius has argued against legitimate interests for cookies used for behavioural targeting.[482] In his opinion, behavioural targeting would not satisfy the necessity and proportionality principle linked to the legitimate interest, since contextual advertisement would provide a less

[476] ibid.
[477] see GDPR Articles 9(2) and 22(2).
[478] European Data Protection Board, 'Statement of the EDPB on the Revision of the EPrivacy Regulation and Its Impact on the Protection of Individuals with Regard to the Privacy and Confidentiality of Their Communications' (2018) 1 and 3 <https://edpb.europa.eu/our-work-tools/our-documents/drugi/statement-edpb-revision-eprivacy-regulation-and-its-impact_en> accessed 7 May 2020.
[479] ibid 1.
[480] Jennifer Baker, 'Critics on Croatia's EPrivacy Proposal: Legitimate Interest Provisions Not Legitimate' (25 February 2020) <https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate/> accessed 7 May 2020.
[481] ibid.
[482] Borgesius (n 47) 168.

intrusive means to market products as it does not entail tracking people's online behaviour.[483] Contextual advertisement means marketing such products or services that fit within the website's content.[484] For example, advertising clothes and accessories on websites about fashion. Additionally, in his opinion, it is technically possible to conduct behavioural targeting without large-scale data collection.[485] However, since most ad network agencies are involved in this kind of data collection it would not satisfy the legitimate interest ground, because it could be considered disproportionate.[486]

Professor Moerel has also advocated for this interpretation that behavioural targeting across websites would not satisfy the balancing of interest tests and hence consent would be more appropriate legal basis.[487] Nevertheless, in her opinion, 'collection of data by cookies for purposes of website analytics, fraud prevention, legal compliance, first party marketing on the site that is visited, should pass the legitimacy test'. [488] However, in contrast to the view of the Croatian Presidency, she does seem to be of the opinion that profiling could rely on the legitimate interest ground. This is inferred from her statement that states the following: 'Personal data may be collected, used (which will include profiling), merged, transferred and destroyed if there is a "legitimate interest of the controller which does not outweigh the privacy rights of the individuals'".[489] Though, this is subjected to the outcome of the balancing of interest test, it is interesting that she thinks that profiling could pass the test but not behavioural targeting, although behavioural advertisement is one of the uses of profiling.[490] Though, the proposed revision does prohibit legitimate interest as a legal basis if the information is used to create an individual profile, it does not explicitly mention online tracking or behavioural advertising. Thus, it is interesting to see whether this will be clarified in the draft.

[483] ibid.
[484] see for example ibid.
[485] ibid 168, 169.
[486] ibid.
[487] Lokke Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' (Lecture at Tilburg University, 14 February 2014) 58 <https://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf> accessed 2 March 2020.
[488] ibid.
[489] ibid 55.
[490] see for example Emmanuel Benoist, 'Collecting Data for the Profiling of Web Users' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) 172; Meike Kamp, Barbara Körffer and Martin Meints, 'Profiling of Customers and Consumers - Customer Loyalty Programmes and Scoring Practices' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) 201; Clifford (n 48) 194.

Despite the heavy criticism, there are also those who see the positive side in introducing the legitimate interest ground, such as Eduardo Ustaran, the Global Co-Head of Hogan Lovells Privacy and Cybersecurity Practice. He stated that:

> I personally think that after so many years of flawed cookie consent, it is a productive thing to do to introduce another approach into the legislative debate. My view is that 'legitimate interests' is misunderstood and underrated as a regulatory mechanism to protect our privacy.[491]

This thesis applauds the EU Council Presidency for introducing a new possible legal basis to the use of cookies as consent has been heavily criticized as discussed above and may therefore not be the appropriate legal basis for cookies in all circumstances. Whether or not this new suggested legal basis for cookies will be able to tackle better the issues surrounding consent and provide better control and transparency for users remains to be seen.

[491] Baker (n 479).

7 Conclusion

The internet is a cyber space that enables people to connect and access a lot of free information and services in exchange for their personal data. Many websites use cookie technology to collect information about their visitors and users. Cookies can be used for multiple purposes, such as, remembering user's preferences, tracking the user's online behaviour, create online user profiles and provide targeted advertisement based on such profiling. Hence, they can be privacy invasive.

As data is the 'world's most valuable resource' in the 21st century,[492] data protection has become a pivotal topic in today's world and it has received prominence, especially in the EU as a result of the GDPR, which imposes high data protection requirements and safeguards. Processing of personal data must be lawful as it interferes with the fundamental human rights to privacy and data protection established under the Charter. Obtaining data subject's consent is one of the legal bases under Article 6 of the GDPR that legitimizes processing of personal data. The EU data protection regime has generally relied on the notion of consent accompanied by the principle of transparency as a tool to protect internet user's data obtained through cookies as seen from Article 5(3) of the ePrivacy Directive.

This thesis has examined whether or not the traditional model of consent and notice is the appropriate legal basis for cookies and concluded that this might not always be the case. The research question was divided into two parts. The first part concerned whether consent and notice are an effective tool in providing control and protection to individuals with respect to personal data processed through internet cookies. The second part of the research question concerned whether the GDPR and the ePrivacy Directive provide clear and harmonised rules on cookie consents and notices.

In terms of the first question, this thesis has shown that consent and notice, though they might be in theory good ideas, do not really work in practice, especially when it comes to website cookies. First of all, if consent is not valid, in other words, it does not meet the requirements of freely given, specific, informed and unambiguous, then consent is an illusory tool that fails

[492] 'The World's Most Valuable Resource Is No Longer Oil, but Data' *The Economist* (6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 6 May 2020.

to give users control over the use of their data. Hence, meeting all of the consent elements can be difficult in itself.

Considering the substantial use of the internet in modern society and its significance in people's lives, it could be considered that consent is rarely freely given, since there is always going to be an imbalance of power between the internet user and the website provider, especially with regard to big corporations like Google and Facebook. Furthermore, users can suffer from social pressure or influence due to many of their friends and peers being in the online community, sharing and connecting with each other and they do not want to be the odd one left out. It might also be difficult to make the consent request specific, since companies themselves might not even know what kind of future uses it can make of the collected personal data.

Companies face also difficulties in making clear and comprehensive privacy and cookie notices required under the GDPR. Thus, if the information given to data subjects prior to consenting is lacking or is difficult to understand, then it is debatable whether the data subject has been able to make an informed decision. Furthermore, though the GDPR has clarified that unambiguous indication means active behaviour from the data subject, there seems to be some websites who still continue with opt-out methods. Moreover, there is some ambiguity between the difference of expressing regular consent versus explicit consent.

Secondly, it has been discussed in this thesis that user's decision making on whether or not to consent to the processing of his or her personal data is burdened by many factors including, inter alia, user's bounded rationality, different types of biases, information asymmetry and transactions costs, as well as different paradoxes. Furthermore, the technological complexity of the internet and cookies is an additional obstacle to user's capacity to understand and make an informed decision. Users are also generally bombarded with so many cookie consent requests daily that it has resulted in click fatigue. Therefore, the conclusion to the first part of the research question is that cookie consent and notice practices under the current data protection framework do not provide effective control and protection to individuals when processing personal data obtained via internet cookies.

This thesis is, however, not of the opinion that consent should be disregarded altogether with respect to cookies, but that the consent mechanisms should be improved in order to be more effective and provide better control. The thesis recognises that cookie consent can be relevant

for certain types of cookie usage, such as, analytics and behavioural advertising. Nevertheless, the legislators should look into other legal bases as well, such as, the legitimate interest ground, especially when it comes to necessary cookies, which are already exempted from consent under the ePrivacy Directive.

Legitimate interest could also be used for contextual advertising, in which case the website would still gain finance through advertisement, even if the user rejects behavioural advertising cookies, but through less invasive means. For behavioural advertising consent might be more appropriate, since it is more invasive and thus the user should be able to choose whether he or she accepts this kind of processing. Websites should, however, explain clearly what behavioural advertisement actually entails in practice, especially with respect to third party advertisement. Furthermore, notice methods should be improved, such as, using more layered information or even more innovative notices like visceral notices.

With regard to the second question, this thesis has used concrete examples from two sectors, in order to show the difference between law in books and law in action. The examples were used to show the different interpretations of cookie consents and notices in practice in the legal and public sector, despite harmonization attempts by the GDPR and the ePrivacy Directive. As seen from the practical examples, many websites tend to use cookie consent as a precaution, even in cases where consent might not be needed, in other words, where the cookies could fall under the consent exemptions, especially with respect to necessary cookies. In these cases, the websites have not given much choice to the user but to accept the necessary cookies. Thus, in these circumstances it is questionable whether another legal basis might be more suitable, such as, the legitimate interest ground. Alternatively, the notice should better clarify that these types of cookies are allowed under EU law irrespective of user's consent.

Around half of the websites examined in this thesis seemed to have consent mechanisms in place, which could be considered compliant with the EU data protection laws. The cookie practices will inevitably vary depending on what type of cookies are used and for what purposes. Nevertheless, the rules on cookie consents and notices seem to lack consistent interpretation and understanding even from the legal sector and the national data protection authorities.

Additionally, as data protection and cookies were previously governed by directives rather than regulations one of the reasons for different approaches to cookie consents in Member States was that each Member State had to implement the directives on national level. Hence, this allowed them more leeway in deciding what kind of cookie consent constituted valid consent in their eyes. The GDPR has brought some harmonization due to being directly applicable to all EU Member States and it has also clarified the general requirements of consent. Nevertheless, as cookies are still governed by a directive, the approach to cookie consent is not harmonised, due to differences in national implementations of the ePrivacy Directive. This issue can be overcome once the proposed ePrivacy Regulation comes into force as it will be directly applicable to all Member States like the GDPR, without the need for any national implementation. Nonetheless, the conclusion to the second part of the research question is that the GDPR and the ePrivacy Directive have failed to harmonise cookie consents and notices.

The proposed ePrivacy Regulation has the opportunity to clarify and facilitate harmonization in terms of cookie practices. Nevertheless, many gaps remain open, such as, the lawfulness of cookie walls. The newest revised draft by the Croatian Presidency introduced legitimate interest as an alternative legal basis for the use of cookies alongside consent. Though, this introduction has received criticism, this thesis supports the EU Council Presidency for its initiative, especially since consent might not always be the appropriate legal basis for cookies. Whether or not the legitimate interest ground will be established as an official alternative legal basis to consent for cookies and able to provide better protection and control to internet users remains to be seen.